Abgeordnetenhaus von Berlin **Drucksache 13 / 1721**

13. Wahlperiode

Vorlage – zur Kenntnisnahme –

über **Stellungnahme des Senats**
zum Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1996

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

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

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

Bericht des Berliner Datenschutzbeauftragten für 1996

und

Stellungnahme des Senats

1. Rechtliche Rahmenbedingungen

1.1 Deutschland und Europa

Informationelle Selbstbestimmung – ein alter Hut?

Im vergangenen Jahr war es 25 Jahre her, daß eine Forschergruppe um den Rechtswissenschaftler Prof. Dr. Wilhelm Steinmüller an der Universität Regensburg dem Bundesministerium des Innern ein Gutachten zu *„Grundfragen des Datenschutzes"* vorgelegt hat[1]. Dieses Gutachten war die Grundlage für die Gestaltung des künftigen Bundesdatenschutzgesetzes. Insbesondere enthielt die Ausarbeitung den Gedanken, daß das Grundgesetz „das Selbstbestimmungsrecht des Bürgers über sein informationelles Personenmodell"[2] garantiere. Hieraus hat das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung abgeleitet, dessen Anerkennung im *„Volkszählungsurteil"*[3] einen über die Bedeutung des ursprünglichen Datenschutzgesetzes weit hinausgehenden Wandel in der rechtlichen Bewertung der Verarbeitung personenbezogener Daten bewirkte. Der Regelungsbedarf für die Datenverarbeitung staatlicher Stellen, aber auch von Privatunternehmen wurde auch von jenen nicht mehr in Zweifel gezogen, die zuvor dem Gedanken des Datenschutzes zweifelnd oder gar ablehnend gegenüberstanden. Gerade in den Bereichen, in denen Informationseingriffe gravierend sein können, war der Bedarf besonders groß.

Vor diesem Hintergrund ist es erstaunlich, daß in den beiden Bereichen, die die staatliche Eingriffsverwaltung in besonderer Weise repräsentieren, nämlich der Strafverfolgung sowie der Finanzverwaltung, bis heute keine angemessenen Datenschutzregelungen in Kraft sind. Vielmehr scheinen im Gegenteil gerade hier diejenigen Kräfte wieder Raum zu gewinnen, die dem Datenschutz nicht nur ablehnend gegenüberstehen, sondern die darüber hinaus der von rechtsstaatlichen Einschränkungen befreiten Verarbeitung personenbezogener Daten das Wort reden.

Für die *Strafverfolgung* wird dies besonders deutlich an dem bereits längst in Vergessenheit gewähnten Slogan *„Datenschutz ist Täterschutz"*, der im vergangenen Jahr wieder zunehmend häufig auch aus dem Munde verantwortlicher Politiker zu hören war. Der Bayerische Landesbeauftragte für den Datenschutz, der die Belange der Sicherheitsbehörden im Kreise der Datenschutzbeauftragten durchaus im Auge hat, hat diese Formulierung jüngst als einen „Kampfbegriff an der Grenze zur Verleumdung" bezeichnet[4]. Abgesehen davon, daß das informationelle Selbstbestimmungsrecht ein Menschenrecht ist, das selbstverständlich auch Straftätern und erst recht Unverdächtigen im Strafverfahren zusteht, suggeriert diese Behauptung, die datenschutzrechtlichen Regelungen behinderten die Ermittlungsarbeit auf inakzeptable Weise.

An den Regelungen in der Strafprozeßordnung (StPO) kann das nicht liegen: Diese enthält nach wie vor in § 163 nur eine allgemeine Aufgabenzuweisung zur „Erforschung" von

Auf welche „Kräfte", die der von rechtsstaatlichen Einschränkungen befreiten Verarbeitung personenbezogener Daten das Wort reden, sich der Berliner Datenschutzbeauftragte bezieht, ist für den Senat nicht erkennbar. Tatsache ist, daß mit zahlreichen Strafprozeßrechtsnovellen (z.B. Entwurf eines Justizmitteilungsgesetzes – Drs. 13/470; Entwurf eines Strafverfahrensänderungsgesetzes 1996 – BR-Drs. 961/96; des Strafverfahrensänderungsgesetzes zur DNA-Analyse [„genetischer Fingerabdruck"] – Drs. 13/667) dem Umstand Rechnung getragen wird, daß datenschutzrechtliche Regelungen auch im Bereich des Strafverfahrens Geltung beanspruchen. Allerdings sind dabei die Besonderheiten des Strafverfahrens zu beachten.

Die Bundesregierung führt dazu in der Begründung zum Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz – JuMiG – Drs. 13/4709 S. 16) aus: „Die Grundsatzaussagen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung sind in allen Bereichen, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, zu beachten. ... Im Hinblick auf die Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person muß der einzelne ... Beschränkungen dulden soweit dies im überwiegenden Allgemeininteresse liegt (BVerfGE 65, 1, 43 f.; ...). Dies trifft in besonderem Maße bei Daten des einzelnen zu, die nicht nur den Bereich seiner privaten Lebensgestaltung, sondern sein soziales Verhalten betreffen und unter diesem Blickwinkel seiner ausschließlichen Verfügungsmöglichkeiten entzogen sind. Insbesondere strafrechtliche Verhaltensweisen betreffen nicht nur den privaten Lebensbereich des einzelnen, sondern berühren auch Belange der Allgemeinheit (BVerwG, NJW 1990, 2765, 2766)."

1 Bundestags-Drucksache (BT-Drs.) VI/3826, Anlage 1
2 aaO S. 88
3 Entscheidungen des Bundesverfassungsgerichts (BVerfG) 65, 1 ff.
4 Süddeutsche Zeitung v. 17.1.97
5 vgl. unten 4.4.3

Bericht des Berliner Datenschutzbeauftragten	Stellungnahme des Senats

Straftaten sowie in § 161 eine dem Wortlaut nach unbeschränkte Amtshilfevorschrift, deren Grenzen etwa im Bereich besonderer Amts- und Berufsgeheimnisse erst in die Vorschrift hineininterpretiert werden müssen. Lediglich einige spezielle Datenschutzvorschriften insbesondere im Sozialgesetzbuch enthalten Bestimmungen, die die zulässigen Auskünfte auch gegenüber Strafverfolgungsbehörden beschränken. Diese waren auch von Anfang an prompt Gegenstand heftigster Kritik sowie von Bemühungen, diese Beschränkungen wieder zurückzudrängen oder gar aufzuheben[5]. Im übrigen beziehen sich die Klagen häufig auf Auskunftsverweigerungen, bei denen sich die befragten Stellen zu Unrecht auf den Datenschutz berufen.

Es liegt in der Natur der Sache, daß insbesondere im strafrechtlichen Ermittlungsverfahren, das zunächst vorrangig – ggf. auch zugunsten des Beschuldigten – der Wahrheitsermittlung dient, andere Maßstäbe gelten müssen, als bei rein verwaltungsmäßigen oder privatrechtlichen Vorgängen. Die Beratungen zu den Gesetzesnovellen dienen der Herstellung einem angemessenen Interessenausgleichs. Aussagen wie „Datenschutz ist Täterschutz“ macht sich der Senat dabei nicht zu eigen.

Der kurz vor Ende des Jahres von der Bundesregierung in das Parlament eingebrachte Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts *Strafverfahrensänderungsgesetz 1996*-(StVÄG 1996)[6] enthält zwar eine Reihe detaillierter Bestimmungen zur Nutzung personenbezogener Daten, läßt aber ebenfalls eine klare, auf die informationelle Selbstbestimmung orientierte Zielrichtung nicht erkennen. Vielmehr werden die Befugnisse der Strafverfolgungsbehörden deutlich ausgeweitet: Die Formulierung, die Polizeibeamten seien berechtigt, „Ermittlungen jeder Art vorzunehmen”, ist mit der informationellen Selbstbestimmung, die eine normenklare Aussage verlangt, auf keinen Fall mehr vereinbar[7].

Zum Entwurf eines Strafverfahrensänderungsgesetzes 1996 wird auf die Stellungnahme zu 4.3.1 „Justiz“ („Strafprozeßordnung“) verwiesen.

Während bei der Justiz, wenn auch spät und unzureichend, zumindest das Bestreben erkennbar ist, durch eine Anpassung der StPO an die formalen Erfordernisse des Datenschutzes für die Strafverfolgung eine verfassungsmäßige Rechtslage zu schaffen, ist ein entsprechender Wille in der *Finanzverwaltung* nicht vorhanden. Seit vielen Jahren mahnen die Datenschutzbeauftragten die Aufnahme datenschutzgerechter Bestimmungen in die Abgabenordnung (AO) an, das Verfahrensrecht der Steuerverwaltung. Entsprechende Vorschläge wurden bislang nicht aufgegriffen. Um einen Fortschritt zu erzielen, wurde eine Erörterung zwischen Datenschutzbeauftragten und den sogenannten „AO-Referenten” angesetzt. Diese verlief völlig erfolglos. Nicht nur, daß die Ministerialbeamten die Vorschläge der Datenschutzbeauftragten im einzelnen ablehnten; vielmehr wurde das geradezu archaische Argument vertreten, die Existenz des Steuergeheimnisses mache es überflüssig, überhaupt Datenschutzregelungen zu erlassen. Die Beamten gingen so weit zu behaupten, die Forderung, durch gesetzliche Regelungen mehr Transparenz für den Steuerpflichtigen zu schaffen, gehe ins Leere, da die Bürger das Gesetz sowieso nicht lesen würden. Es ist kaum faßbar, daß bundesweit in einer Ministerialbürokratie den Bürger derart geringschätzende Äußerungen möglich sind.

Entgegen der Darstellung des vorliegenden Berichts steht der Senat insgesamt Vorschlägen zur Fortentwicklung der Abgabenordnung (AO) für den Bereich des Datenschutzes positiv gegenüber. Der Auffassung des Datenschutzbeauftragten kann aber nicht gefolgt werden, wenn behauptet wird, daß die AO insgesamt den verfassungsrechtlichen Anforderungen zur Wahrung des Persönlichkeitsrechts der Betroffenen bei der Verarbeitung und Nutzung der personenbezogenen Daten nicht genügt.

Weder das Bundesverfassungsgericht noch der Bundesfinanzhof haben bisher Vorschriften der AO aus datenschutzrechtlicher Sicht beanstandet. Vielmehr wurden Vorschriften der AO wie beispielsweise das Steuergeheimnis (§ 30 AO), die Auskunfts- und Anzeigepflichten sowie die Ermächtigung zur Ausschreibung von Kontrollmitteilungen (§§ 93 Abs. 1, 194 Abs. 3, 208 Abs. 1 AO) ausdrücklich oder inzident für verfassungsgemäß angesehen. Wenn daher die Vorschriften der AO auch insgesamt unter datenschutzrechtlichen Gesichtspunkten verfassungskonform sind, so ist allenfalls eine Präzisierung bestimmter Vorschriften möglich, soweit dies eine wirkliche Verbesserung in datenschutzrechtlicher Hinsicht bedeutet.

Diese Befunde lassen darauf schließen, daß derzeit offensichtlich andere Prioritäten als die der Sicherstellung der Grundrechte gelten. Diese Vermutung wird gestärkt durch eine weitere Beobachtung: Angesichts schwieriger Probleme in der Gesellschaft nimmt offensichtlich die Bereitschaft zu, in mehr und mehr Bereichen Lösungen mit Mitteln zu suchen, die bisher *polizeilichem Denken* vorbehalten waren.

So wird die *„Rasterung”*, also die systematische Durchforstung ganzer Datenbestände und deren Abgleich mit anderen Daten, zu einem vielfach begehrten Instrument der Verwaltungstätigkeit. Ursprünglich als unbestritten eingriffsintensives Mittel der polizeilichen Fahndung

Aus dieser Sicht heraus hat das Bundesministerium der Finanzen zusammen mit den für Fragen der Abgabenordnung zuständigen Vertretern der obersten Finanzbehörden der Länder eine Vielzahl von Vorschlägen zur datenschutzrechtlichen Verbesserung der AO, die der Bundesbeauftragte für den Datenschutz im Einvernehmen mit den Landesbeauftragten für den Datenschutz an das Bundesministerium der Finanzen herangetragen hat, geprüft und gegenüber dem Bundesbeauftragten für den Datenschutz mit Schreiben vom 11. März 1997 (IV A 4 – S 0030 – 3/97) Stellung genommen. Eine Ablichtung dieses Schreibens ist zwischenzeitlich von der Senatsverwaltung für Finanzen an den Berliner Datenschutzbeauftragten weitergeleitet worden. Die Prüfung der einzelnen Vorschläge ist zum Teil noch nicht

6 Bundesrats-Drucksache (BR-Drs.) 961/96
7 vgl. unten 4.3.1
8 vgl. unten 4.4.3
9 vgl. unten 4.2.1

entwickelt, das ohne schwere Not nicht einsetzbar galt, wird dieses nunmehr verharmlosend „Datenabgleich" genannte Verfahren in allerlei Situationen als Allheilmittel betrachtet. Die Befugnis der Sozialhilfebehörden, derartige Rasterungen durchzuführen, wurde bereits vor Jahren in das Bundessozialhilfegesetz hineingeschrieben und im vergangenen Jahr noch verschärft[8]. Nur das Zögern des Bundesgesundheitsministeriums, eine entsprechende Verordnung zu erlassen, und technische Probleme vor Ort verhindern bisher eine flächendeckende Rasterung von Sozialdaten. Der Drang der Rundfunkanstalten, ihr Gebührenaufkommen dadurch zu erhöhen, daß alle Veränderungen im Melderegister mit den Beständen der Gebühreneinzugszentrale (GEZ) „abgeglichen" werden[9], lieferte im vergangenen Jahr in Berlin ein beredtes Beispiel, mit welchen Nachahmern noch zu rechnen ist.

Eine Steigerung erhält diese Tendenz, wenn eine zweite polizeiliche Methode in das Verfahren einbezogen wird: die *erkennungsdienstliche Behandlung* insbesondere in der Form der Daktyloskopie, der Abnahme und Auswertung von Fingerabdrücken. Ebenfalls früher in strafrechtlichen Ermittlungsverfahren noch mit Zurückhaltung genutzt[10], wird sie zunehmend in ganz anderen Bereichen gefordert. Bereits vor zwei Jahren wurde bundesweit entgegen dem klaren Votum der Datenschutzbeauftragten die Möglichkeit der vollständigen daktyloskopischen Erfassung der Asylbewerber eingeführt, im vergangenen Jahr war über den (bislang gescheiterten) Versuch der Berliner Innenverwaltung zu berichten, alle bosnischen Kriegsflüchtlinge entsprechend zu erfassen; seit einiger Zeit wird die Erhebung entsprechender Daten von allen ausländischen Sozialhilfeempfängern diskutiert – das Bundeskriminalamt, das als einziges über die entsprechenden bundesweit einsetzbaren Techniken verfügt, als Erfüllungsgehilfe der Sozialämter!

Auch der Aufbau *zentraler Vorratssammlungen* personenbezogener Daten in einzelnen Bereichen hat in den kriminalpolizeilichen Täter-/Tatsammlungen sein Vorbild; der einstige Präsident des Bundeskriminalamtes war viel Kritik ausgesetzt, als er den Aufbau derartiger Verfahren (mit sozialtherapeutischer Zielrichtung) in Erwägung zog – heute scheut man sich nicht einmal davor, derartige Sammlungen für Wanderzirkusse einzurichten[11].

Es ist nicht verwunderlich, daß auch die Privatwirtschaft diesen Trend aufnimmt. Das „Scoring" bei der Kreditkartenvergabe oder der Datenhunger von Vermietern[12] weisen in die Richtung Rastern, über Daktyloskopie als Sicherheitsinstrument wird im Rahmen „biometrischer" Methoden immer lauter nachgedacht, Vorratsspeicherungen in Form „schwarzer Listen" werden in immer mehr Bereichen angelegt.

Wo führt dieser Weg hin? Jedenfalls nicht in eine freiheitlichere Gesellschaft, die wir alle anstreben sollten, sondern mit größerer Wahrscheinlichkeit in eine Gesellschaft, in der – wie es das Bundesverfassungsgericht klassisch formuliert hat – der Bürger von seinen Freiheitsrechten keinen Gebrauch mehr macht, weil er sich vom Staat und, man wird heute ergänzen müssen, von privaten Unternehmen – beobachtet fühlt.

Bundes- und Europarecht

Die bedeutendsten Neuregelungen des Bundesrechtes im vergangenen Jahr finden sich im *Telekommunikationsrecht*: Mit abgeschlossen.

Es ist richtig, daß der Bundesgesetzgeber im Ausländer- und Asylverfahrensrecht Regelungen geschaffen hat oder zu schaffen beabsichtigt, die die erkennungsdienstliche Behandlung ermöglicht oder für bestimmte Personengruppen zwingend vorschreibt. Unzutreffend ist dagegen die Behauptung, es bestehe „die Möglichkeit der vollständigen daktyloskopischen Erfassung der Asylbewerber". Asylbewerber mit einer unbefristeten Aufenthaltsgenehmigung oder Personen vor Vollendung des 14. Lebensjahres werden nicht erkennungsdienstlich behandelt (§ 16 Abs. 1 AsylVfG).

Im übrigen dienen gerade die angesprochenen Befugnisnormen der Bekämpfung von Mißbrauch, da etwa bei Asylbewerbern oder sonstigen Flüchtlingen eine Vielzahl von Personen über keine Ausweisdokumente verfügt oder dies zumindest behauptet.

[10] Entscheidungen des Bundesverwaltungsgerichts (BVerwG) 26, 169 ff.
[11] § 16 Abs. 5 S. 2 Entwurf eines Gesetzes zur Änderung des Tierschutzgesetzes, BR-Drs. 763/96
[12] vgl. unten 4.4.4

dem Inkrafttreten der dritten Stufe der „Postreform" mit dem Telekommunikationsgesetz (TKG)[13] ist nunmehr eine (vorläufig?) endgültige Regelung der Telekommunikation erreicht, die zum Teil zufriedenstellende, zum Teil problematische Bestimmungen zum Datenschutz enthält. Ergänzt wird das TKG durch die neue Telekommunikationsdienstunternehmen-Datenschutzverordnung (sic!) (TDSV), die allerdings noch auf der alten Rechtslage aufsetzt[14].

Von der Bundesregierung eingebracht wurden im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (IuK-Dienste-Gesetz) der Entwurf eines Teledienste-Datenschutzgesetzes sowie eines Gesetzes zur digitalen Signatur, die das auf den Netzbetrieb beschränkte TKG um Regelungen im Bereich der Telekommunikationsdienste ergänzen[15].

In Kraft getreten sind mehrere Gesetze auf dem Gebiet des *Sozialrechts* mit einer Reihe von Regelungen zu Datenverarbeitung und Datenschutz, so das neue 7. Buch des Sozialgesetzbuches zum Recht der gesetzlichen Unfallversicherung (SGB VII), ein Gesetz zur Änderung des Asylbewerberleistungsgesetzes, das Mitteilungspflichten zwischen Ausländerbehörden und Sozialleistungsträgern vorsieht, sowie eine Reform des Sozialhilferechts u.a. mit dem bereits erwähnten Ziel, den Datenabgleich zwischen Sozialleistungsträgern zu erleichtern[16]. In parlamentarischer Beratung befindet sich der Entwurf eines 3. Buches des Sozialgesetzbuches zur Einordnung der Arbeitsförderung (SGB III), die Bemühungen, auch das Recht der Rehabilitation und Eingliederung Behinderter in das SGB einzufügen (SGB IX), sollen wieder aufgenommen werden.

Änderungen des *Stasi-Unterlagen-Gesetzes* brachten einen Ausschluß von Auskünften über Tätigkeiten, die vor 1976 stattfanden, aber auch eine Verlängerung der Frist, bis zu der die alten Datenbestände des Zentralen Einwohnerregisters der DDR genutzt werden können, bis 31. Dezember 2005. Der letzte Punkt war vor Jahren Gegenstand intensiver Auseinandersetzungen zwischen den Datenschutzbeauftragten und den interessierten Behörden[17]; auch die Möglichkeit, die eigenen personenbezogenen Daten in den Stasiunterlagen anonymisieren bzw. löschen zu lassen, wurde um zwei Jahre auf Anfang 1999 hinausgeschoben.

Veränderungen für alle Verkehrsteilnehmer wird das Gesetz zur Änderung des *Straßenverkehrsgesetzes* bringen, mit dem vor allem ein Zentrales Fahrerlaubnisregister eingeführt werden soll; das Gesetz wird derzeit im Bundestag beraten[18].

Das datenschutzrechtlich für die nächsten Jahre bedeutsamste Vorhaben ist noch nicht auf den Weg gebracht: die Umsetzung der *EU-Richtlinie zum Datenschutz* aus dem Jahr 1995[19]. Die Datenschutzbeauftragten haben sich ausführlich mit der Frage auseinandergesetzt, welche Änderungen des Bundesdatenschutzgesetzes nicht nur unerläßlich sind, sondern auf welche Weise das deutsche Recht insbesondere auch vor auf dem Hintergrund neuer technischer Gegebenheiten weiterentwickelt werden sollte[20]. Leider ist den Verlautbarungen aus dem Bundesinnenministerium zu entnehmen, daß man dort eine minimalistische

Der Senat wird über die Notwendigkeit von Änderungen des Bundesdatenschutzgesetzes und sein Stimmverhalten im Bundesrat entscheiden, sobald der entsprechende Gesetzentwurf der Bundesregierung zur Anpassung des Bundesdatenschutzgesetzes (BDSG) an die EU-Richtlinie zum Datenschutz vorliegt.

13 vgl. unten 4.7.1
14 vgl. unten 4.7.1
15 vgl. unten 4.7.1
16 vgl. unten 4.4.3
17 vgl. JB 1990, 2.1; 1991, 2.2; 1992, 3.2
18 vgl. unten 4.2.4
19 Amtsblatt der EG (ABLEG) Nr. L 281 vom 23. November 1995, S. 31
20 vgl. Anlage 2.2

Lösung anstrebt[21] – damit würde man erneut eine Chance verpassen, die Grundrechte der Bürger zu stärken.

Von zentraler Bedeutung wird die Regelung des *Exports personenbezogener Daten* ins Ausland sein. Die EU-Richtlinie geht davon aus, daß die Datenübermittlung im Europäischen Binnenmarkt (also z.B. von einem Berliner Unternehmen an ein Unternehmen in Österreich) wie eine Datenübermittlung im Inland zu behandeln ist, soweit die Richtlinie in den beiden beteiligten Mitgliedstaaten umgesetzt worden ist. Dieser Datenexport darf jedenfalls nicht mehr aus Gründen des Datenschutzes unterbunden werden.

Für den *Export in außereuropäische Staaten (Drittländer*) verpflichtet die Richtlinie die Mitgliedstaaten der Union, die grenzüberschreitende Datenübermittlung nur in solche Länder zuzulassen, in denen ein *angemessenes Datenschutzniveau* gewährleistet ist (Artikel 25). Diese Frage hat uns bereits im vorigen Jahr im Zusammenhang mit der BahnCard intensiv beschäftigt[22]. Die dort gefundene *Vertragslösung* wurde auf der 19. Internationalen Datenschutzkonferenz in Ottawa im September 1996 vorgestellt und diskutiert. Es bestand Einvernehmen darüber, daß eine vertragliche Sicherstellung des angemessenen Datenschutzniveaus im Empfängerland außerhalb der Europäischen Union nur ausnahmsweise in Frage kommen kann. Vertragliche Standards können die nationale Gesetzgebung immer nur ergänzen, nie jedoch ersetzen. Andererseits wird sich ein angemessenes Datenschutzniveau nicht kurzfristig durch allgemeine oder sektorielle Datenschutzgesetzgebung in allen Ländern der Erde sicherstellen lassen, die personenbezogene Daten aus Europa importieren. Es ist weder möglich noch akzeptabel, in der Übergangszeit die Datenflüsse entweder ganz zu unterbinden oder ohne jede Sicherung zuzulassen. In dieser Phase können bereichsspezifische vertragliche Lösungen – wie im BahnCard-Fall geschehen – die Rechte der vom Datenexport betroffenen Bürger angemessen schützen. Dementsprechend hat die Arbeitsgruppe „Internationaler Datenverkehr" des Düsseldorfer Kreises unter unserem Vorsitz *Leitlinien zur Übermittlung personenbezogener Daten in Länder ohne angemessenes Datenschutzniveau* erarbeitet, die der Düsseldorfer Kreis zustimmend zur Kenntnis genommen hat[23].

In *Europa* konzentrierten sich die Aktivitäten nach dem Inkrafttreten der allgemeinen Datenschutzrichtlinie auf die Schaffung datenschutzrechtlicher Regelungen bei einzelnen Spezialmaterien („horizontaler Datenschutz"), etwa in der erfreulicherweise von Rat und Kommission als Gemeinsamer Standpunkt beschlossenen Richtlinie zum Datenschutz in digitalen *Telekommunikationsnetzen* (hinter der sich auch Regelungen für die Telekommunikation im allgemeinen verbergen)[24].

Die *Arbeitsgruppe nach Artikel 29* der allgemeinen Datenschutzrichtlinie hat ihre Arbeit aufgenommen und in mehreren Sitzungen Einzelfragen der Harmonisierung des europäischen Datenschutzrechts erörtert.

Zum Übereinkommen über die Einrichtung eines *europäischen Polizeiamtes* vom Juli 1995 (EUROPOL-Konvention) liegt ein Entwurf eines Übernahmegesetzes vor[25], zum Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich (ZIS-

[21] vgl. die Rede von Staatssekretär Werthebach bei der 20. Datenschutzfachtagung (DAFTA) 1996 „20 Jahre Bundesdatenschutzgesetz – vom Stiefkind zum Exportmodell"
[22] Jahresbericht (JB) 95, 3.1
[23] s. Anlage 3
[24] s. unten 4.7.1
[25] s. unten 4.1.1

Übereinkommen)[26] vom gleichen Datum wird der Entwurf eines Zustimmungsgesetzes erwartet. Die von der Bundesregierung lange verschleppte Übernahme der EG-Rahmenrichtlinie Arbeitsschutz u.a. mit Regelungen zu Bildschirmarbeitsplätzen[27] erfolgte endlich im Dezember auf der Grundlage der Neufassung des Arbeitsschutzgesetzes in der Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten[28].

Keine wesentlichen Impulse zur Fortentwicklung des informationellen Selbstbestimmungsrechts kamen im vergangenen Jahr von der Rechtsprechung, diese war vielmehr geprägt von der – meist restriktiven – Anwendung von im Grundsatz anerkannten Positionen auf konkrete Fallgestaltungen. So sah das *Bundesverfassungsgericht* weder in der Überprüfung vollständiger Patientenakten durch den Rechnungshof[29] noch im Vergleich von Genomanalysen bei Straftaten aufgrund der Bestimmung des § 81 a StPO (die die Besonderheit dieser Methode in keiner Weise berücksichtigt)[30] oder in der Verwendung des äußerst umstrittenen ICD 10-Codes im Rahmen der Diagnoseverschlüsselung beim Meldeverfahren gegenüber den Krankenkassen[31] einen verfassungswidrigen Verstoß gegen das informationelle Selbstbestimmungsrecht. Lediglich die Bedenken gegen die Befugnisse des Bundesnachrichtendienstes bei der Überwachung des Telefonverkehrs zu Zwecken der Strafverfolgung wurden bestätigt[32], ohne daß es hier bisher zu einer abschließenden Entscheidung gekommen ist.

1.2 Datenschutz in Berlin

Die Grundstimmung in Berlin folgte tendenziell derjenigen im ganzen Bundesgebiet. Auch hier stand im Vordergrund die Behauptung, der Datenschutz behindere die Arbeit der Verwaltung, insbesondere die Strafverfolgung, ungebührlich. In einer Entschließung hat das Abgeordnetenhaus den Senat aufgefordert[33], zu letzterem einen Bericht zu erstellen; der Datenschutzbeauftragte soll Gelegenheit erhalten, hierzu Stellung zu nehmen.

Der Senat von Berlin wird dem Abgeordnetenhaus von Berlin den erbetenen Bericht zuleiten.

Bereits jetzt läßt sich allerdings feststellen: Die ständig wiederholte Behauptung, die organisierte Kriminalität nehme bedrohlich zu und mache deshalb eine Ausweitung der Befugnisse der Strafverfolgungsbehörden – und daraus ergeben sich in der Regel weitere Einschränkungen des informationellen Selbstbestimmungsrechts – erforderlich, läßt sich jedenfalls an den zuletzt vorgelegten Zahlen der *Polizeilichen Kriminalstatistik* (PKS) nicht nachweisen. In dem entsprechenden Kapitel der PKS für das Jahr 1995 wird vielmehr seit 1993 ein kontinuierlicher Rückgang der Fallzahlen festgestellt: Von 5 088 Fällen im Jahr 1993 auf 4 567 Fälle im Jahr 1994 sowie auf 4 233 Fälle im Jahr 1995; die Zahl der ermittelten Tatverdächtigen fiel in diesem Zeitraum von 3 942 auf 3 467. Die Zahl der entwendeten Kraftfahrzeuge fiel geradezu dramatisch: bei der Marke Mercedes-Benz, nicht älter als zwei Jahre, von 801 (1994) auf 233

Im Bericht der Senatsverwaltung für Inneres über die Kriminalitätsentwicklung in Berlin, zuletzt am 3. März 1997 für das Jahr 1996, wurde deutlich hervorgehoben, daß die Polizeiliche Kriminalstatistik (PKS) kein getreues Spiegelbild der in Berlin begangenen Kriminalität ist, sondern nur die der Polizei bekannt gewordenen, von ihr abschließend bearbeiteten und registrierten Straftaten enthält. Der Umstand, daß verübte, aber nicht bekanntgewordene Straftaten (Dunkelfeld) in den verschiedenen Deliktsbereichen deutlich variieren und insofern feststehende Relationen zwischen tatsächlich begangenen und statistisch erfaßten Straftaten nicht zulassen, führt dazu, daß die PKS letztlich nur eine je nach Delikt mehr oder weniger starke Aussage über die Annäherung an die Realität geben kann. Die PKS ist demnach als Beschreibung und Bewertung des Phänomens der Organisierten Kriminalität (OK) nur bedingt geeig-

[26] ENFOCustom 16, Ratsdokument 7256-2-95
[27] Richtlinie 90/270/EWG des Rates v. 29.Mai 1990 über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten/ABlEG Nr.L 156 S. 14
[28] Artikel 3 der Verordnung zur Umsetzung von EG-Einzelrichtlinien zur EG-Rahmenrichtlinie Arbeitsschutz v. 4. 12.96, Bundesgesetzblatt (BGBl.) S. 1843
[29] Recht der Datenverarbeitung (RDV) 1996, 184
[30] Juristenzeitung 1996, 1175
[31] Neue Juristische Wochenschrift (NJW) 1996, 771
[32] Beschluß v. 10. Dezember 1996 Az. 1 BvR 2226/94
[33] Drs. 13/1148

(1995). Auch die immer wieder vorgebrachten Klagen über den Anstieg des Sozialleistungsbetrugs, die auch in Berlin etwa zur bereits erwähnten Forderung nach einer erkennungsdienstlichen Behandlung führten, lassen sich jedenfalls auf die Statistik nicht stützen. Die Zahlen beim „Leistungsbetrug", der Straftat, unter die die entsprechenden Straftaten fallen, sprechen eine andere Sprache: Sie sanken von 1 039 Fällen im Jahr 1992 auf 430 im Jahr 1995. Dies kann nur bedeuten, daß vor allem in der Presse herausgestellte Einzelfälle die Vermutung fördern, daß es zu einem Anstieg dieser Art der Kriminalität gekommen ist, ohne daß das tatsächlich der Fall ist.

Statt auf Grund bestimmter Stimmungen immer neue Ermittlungsmethoden zu fordern und damit den Datenschutz einzuschränken, sollte man sich auch in Berlin darauf konzentrieren, im Rahmen der bestehenden Gesetze (die weit genug sind) Kriminalität gezielter zu bekämpfen.

net, da sich diese gemäß ihrer Definition als deliktsübergreifendes Phänomen darstellt.

OK ist die von Gewinn und Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
b) unter Anwendung von Gewalt oder anderen zur Einschüchterung geeigneten Mittel,
c) unter Einflußnahme auf Politik, Medien, öffentliche Verwaltung, Justiz und Wirtschaft

zusammenwirken.

Die ihr zuzuordnenden Einzeldelikte werden anders als z.B. bei der Wirtschaftskriminalität in der statistischen Erfassung der PKS nicht gesondert gekennzeichnet. Zur Beschreibung dieses Phänomens wird daher auch das nach einem bundeseinheitlichen Erhebungsraster erstellte „Lagebild OK" herangezogen Dieses weist für den engeren Bereich der OK entsprechend des vorgenannten Berichtes für

1993	3.362 Einzelstraftaten,
1994	2.680 Einzelstraftaten,
1995	3.344 Einzelstraftaten und
1996	4.650 Einzelstraftaten

aus. Bei den vom Berliner Datenschutzbeauftragte erwähnten Angaben für 1993 – 1995 handelt es sich um die bei der polizeilichen Fachdienststelle im weiteren Bezug zur OK bearbeiteten Fälle. Die Entwicklung nach dem Lagebild-OK zeigt demnach seit 1994 einen starken Anstieg im Bereich der OK an. Im übrigen verkennt der Berliner Datenschutzbeauftragte die eingeschränkte Aussagekraft der PKS und reduziert die Bedeutung der Organisierten Kriminalität als Gefahr für die Innere Sicherheit auf die bloße Darstellung von Fallzahlen des statistischen Hellfeldes.

Die Organisierte Kriminalität ist entgegen der Diktion des Beitrages des Datenschutzbeauftragten kein spezifisches Berliner Phänomen, sondern eine internationale, komplexe, kriminelle Erscheinungsform, der sowohl nationale als auch internationale Bekämpfungsstrategien entgegengesetzt werden müssen. Insbesondere die Begegnung der Verfestigung von OK-Strukturen auch in Berlin ist vordringliches Ziel polizeilicher Bekämpfungsstrategien und weniger eine Frage der „Fallzahlen". Hierzu gehört sowohl eine auf diese Form hin ausgerichtete spezifische Ausrichtung polizeilicher Arbeit, das Zusammenwirken von Behörden im regionalen, nationalen und internationalen Bereich sowie mit den privaten Akteuren der gewerblichen Wirtschaft wie dem Bausektor, der Entsorgungswirtschaft, der Versicherungswirtschaft, der Automobilindustrie, Kreditkartenunternehmen etc. als auch die gezielte Bekämpfung mit gesetzgeberischen Maßnahmen, wie z.B. mit den OrgKG, dem Geldwäschegesetz und das Verbrechensbekämpfungsgesetz. Insbesondere vor dem Hintergrund, daß sich Europa mehr und mehr als Operationsraum für sowohl weltweit agierende Verbrechersyndikate als auch für west- und osteuropäische OK-Gruppierungen präsentiert, bedarf es auch weiterer gesetzgeberischer Reformen.

Denn die Entwicklung der OK ist gekennzeichnet durch

- zunehmende Internationalisierung der OK-Netzwerke
- steigende Professionalität der OK im europäischen Raum,
- zunehmende regionale Ausdifferenzierung der Kriminalitätsfelder,
- unterschiedliche nationale OK-Bekämpfung im europäischen Raum.

Bericht des Berliner Datenschutzbeauftragten	Stellungnahme des Senats

Dieser OK wirksam entgegentreten zu können, erfordert sowohl die Ausschöpfung des bisherigen rechtlichen Handlungsrahmen als auch die notwendige Ergänzung, um den Strafverfolgungsbehörden die notwendigen Rechtsgrundlagen für erforderliche Eingriffsmaßnahmen zu geben.

Auch die Hinweise im Zusammenhang mit den Aussagen zum Sozialleistungsbetrug bedürfen der Korrektur. Entgegen der Annahme des Berliner Datenschutzbeauftragten wurden und werden die Delikte zum „sonstigen Sozialleistungsbetrug“ *nicht* unter dem Erfassungsmerkmal „Leistungsbetrug“ der PKS statistisch ausgewiesen. Zum „Leistungsbetrug“ werden vielmehr nur die Fälle erfaßt, in denen der Täter eine Be- oder Anzahlung erlangt, indem er arglistig vortäuscht, er werde eine Leistung vollbringen, in Wirklichkeit jedoch nichts leistet bzw. die Ausführung qualitativ nicht den Mindestanforderungen entspricht. Betrugsdelikte zum Nachteil von Sozialbehörden wurden bis einschließlich 1995 in der Straftatenobergruppe „sonstiger Betrug“ der PKS erfaßt. Seit 1996 werden diese gesondert als „sonstiger Sozialleistungsbetrug“ ausgewiesen. Für 1996 waren dies 1.764 Fälle. Die vom Berliner Datenschutzbeauftragten herangezogenen Daten betreffen somit den von ihm angesprochen Sachverhalt überhaupt nicht. Insofern beruht seine Schlußfolgerung auf einer Fehlinterpretation der PKS. Bereits die Anzahl der für 1996 erfaßten Delikte zeigt, daß es sich hierbei nicht um wenige Einzelfälle handelt, bei denen ein Schaden nach der PKS in Höhe von 1,4 Millionen DM erfaßt wurde. Die Pflicht, staatliche Sozialleistungen nur denen und im erforderlichen Umfange zukommen zu lassen, die auch bedürftig sind, gebietet es im besonderen Maße, alle notwendigen Maßnahmen zu ergreifen, um die mißbräuchliche, insbesondere betrügerische Inanspruchnahme, zu verhindern. Dies gilt um so mehr, als auch die für den sozialen Bereich zur Verfügung stehenden finanziellen Mitteln nicht unerschöpflich sind.

Da im vergangenen Jahr eine neue Legislaturperiode einsetzte und der neue Senat im wesentlichen mit Fragen der Haushaltskonsolidierung befaßt war, sind neue *Gesetzesinitiativen* kaum zu verzeichnen. Die Gesetzgebung der vergangenen Jahre hat ohnehin in weiten Bereichen Datenschutzbestimmungen geschaffen (die allerdings durchaus verbesserungsbedürftig sind). Nur das lange angemahnte Sicherheitsüberprüfungsgesetz läßt immer noch auf sich warten, so daß Sicherheitsüberprüfungen in Berlin nach wie vor ohne Rechtsgrundlage durchgeführt werden.

Als Aufgabe für die nächste Zeit steht die Anpassung des Berliner Datenschutzgesetzes an die *EU-Richtlinie* an. Sie entfaltet durchaus auch für die Berliner Verwaltung Wirkung, insbesondere da, wo eine Gemengelage zwischen öffentlich-rechtlichem und privatrechtlichem Vorgehen besteht.

Für seine Entscheidung über die Notwendigkeit von Änderungen des Berliner Datenschutzgesetzes im Hinblick auf die EU-Richtlinie zum Datenschutz wird der Senat zunächst die Rechtsdiskussion im Bund abwarten.

Im Gegensatz zur Gesetzgebung machte im vergangenen Jahr die *Umsetzung des Datenschutzes und die Gewährleistung einer hinreichenden Kontrolle in Berlin* Probleme. Konnte früher davon berichtet werden, daß die Berliner Verwaltung der Umsetzung des Datenschutzes relativ aufgeschlossen gegenübersteht, mehren sich die Fälle, in denen sich einzelne Stellen weigern, die gesetzlichen Vorgaben zu akzeptieren und die gesetzlich vorgeschriebene Zusammenarbeit mit dem Berliner Datenschutzbeauftragten sicherzustellen. Hierzu wird unten noch näher berichtet[34].

Die früher insbesondere von der Innenverwaltung vorgebrachte Befürchtung, die Übertragung der Aufgaben der *Aufsichtsbehörde* für den privaten Bereich auf den

Der Senat übt die Rechtsaufsicht über den Berliner Datenschutzbeauftragten als Aufsichtsbehörde im privaten Bereich aus. Im Jahre 1996 gab es keinen Anlaß, aufsichtlich tätig zu

[34] vgl. unten 5.2.3

Datenschutzbeauftragten werde bei Berliner Unternehmen zu Widerständen und zurückgehender Kooperationsbereitschaft führen, hat sich nicht bestätigt. Vielmehr ist es auch bei stark angestiegenen Fallzahlen im wesentlichen zu einer konstruktiven Zusammenarbeit mit den geprüften Betrieben gekommen; die in der Verwaltung zunehmende Skepsis findet keine erkennbare Entsprechung in der Privatwirtschaft – was natürlich auch mit dem Umstand zu tun hat, daß die Regelungen in diesem Bereich (noch) erheblich großzügiger sind als im öffentlichen Sektor.

Hinzu kommt, daß die Privatwirtschaft zunehmend erkennt, wie wichtig der Datenschutz für die Akzeptanz bestimmter Produkte und Dienstleistungen durch den Kunden ist – eine Erkenntnis, die sich in der öffentlichen Verwaltungsreform erst durchsetzen muß.

werden.

2. Technische Rahmenbedingungen

2.1 Tendenzen und Entwicklungen der Informatio nstechnik

Trends setzen sich fort

Grundsätzlich haben sich in diesem Jahr die Tendenzen weiter fortgesetzt, die bereits seit Jahren an dieser Stelle berichtet wurden:

Die *Miniaturisierung der Computer* schreitet weiter fort. Da die transportablen Systeme mittlerweile eine Größe erreicht haben, bei der eine weitere Verkleinerung ergonomisch keinen Sinn mehr machen würde, wirkt sich der Fortschritt in der Leistungsfähigkeit der Laptops, Notebooks und Handheld-Computer aus. In gleicher Weise wird auch die Leistungsfähigkeit von Chipkarten immer weiter ausgebaut, ohne daß sich an den genormten Größen etwas ändert. Die Verbesserung des *Preis-Leistungs-Verhältnisses* setzt sich ungebrochen fort. Personalcomputer, die im Frühjahr zu den High-End-Produkten zählten, definieren im Herbst des gleichen Jahres den Durchschnitt.

Bei den Bürosystemen spielen Mehrplatzsysteme mit nichtintelligenten Terminals im Vergleich zu *Client-Server-Systemen* keine Rolle mehr. Die reichhaltigen und flexiblen Standard-Anwendungsprogramme der PC-Welt können so mit zentraler Datenhaltung und Softwareversorgung ergänzt und optimiert werden. Herstellergebundene Großsysteme (*„proprietäre Systeme"*) gibt es in der Berliner Verwaltung zwar noch, sie verlieren aber weiter an Bedeutung.

Auch die weiteren Trends, über die wir zuletzt[35] berichtet hatten, setzen sich ungebrochen fort: Weiterentwicklung der multimedialen Anwendungen, vor allem bei der Telekommunikation, weitere Ausbreitung von Outsourcing, das Auslagern von IT-Dienstleistungen in spezialisierte Unternehmen. Das besondere Interesse bei den neuen technologischen Entwicklungen gilt hier jedoch der weltweiten Vernetzung über das Internet und den Chipkarten. Beide Themen stehen für die entgegengesetzten Seiten der technischen Repräsentation der globalen Informationsgesellschaft: das *Internet* als weltweit eng gespannte Infrastruktur und die *Chipkarten* als das individuelle Instrument für die effektive Nutzung der Infrastruktur.

Megamaschine Internet

Während der Gesetzgeber mit dem IuK-Dienste-Gesetz das

[35] JB 1995, 2.1

nationale Recht für den Eintritt in die Informationsgesellschaft vorbereitet, ist auch auf der technischen Seite die Entwicklung weiter vorangeschritten. Die technische Infrastruktur für die zukünftige globale Informationsgesellschaft entwickelt sich mehr und mehr zu einer weltweiten Megamaschine. *Informations- und Kommunikationstechnik* wachsen zusammen. Einzelsysteme werden zu lokalen Netzen zusammengesteckt, lokale Netze an übergeordnete Netze, z.B. Behördennetze, Konzernnetze, Regionalnetze angeschlossen. Alle kommunizieren über das Internet mit dem Rest der Welt. Dieses Szenario ist für viele Anwender längst Realität. Isolierte Systeme werden immer mehr zur Ausnahme. Das Problem der Zukunft ist nicht mehr, wie man sich Informationen verschaffen kann, die man für private und berufliche Zwecke braucht, sondern wie man aus den überbordenden Informationsfluten jene Informationen selektieren kann, die man benötigt, und wie man dazu sicher sein kann, nichts Wesentliches übersehen zu haben.

Die weltweite Megamaschine heißt derzeit noch *Internet*. Daß die zunehmende Kommerzialisierung und Professionalisierung dem Internet den anarchischen Charme der frühen Jahre nehmen wird, dürfte klar sein. Das Internet wird sich ändern, wenn höhere Anforderungen an Sicherheit und Verläßlichkeit, an Kontrollierbarkeit und Transparenz an die weltweite Kommunikation gestellt werden. Die offene Kommunikation über das Internet ist manchen Regierungen ein Dorn im Auge, ob wegen politisch unerwünschter Inhalte oder weil die jeweiligen gesellschaftlichen Toleranzgrenzen und Tabuzonen überschritten werden können.

Die Megamaschine bietet *offene Kommunikationswege*, die kaum zu beschneiden sind. Elektronische Post kann mit Teilnehmern in allen Ländern der Welt ausgetauscht werden, ohne daß Zensoren große Chancen besitzen, sie abzufangen oder zu unterbinden. Informationsangebote aus aller Welt können in Anspruch genommen werden, ohne daß Zensoren und Tugendwächter dem erfolgreich einen Riegel vorschieben können. Sie bietet ferner eine weltweite *Bereitstellung von Ressourcen*, vor allem Daten, Dokumenten, Programmen, in Einzelfällen auch Systemen. Was einmal irgendwo zur Verfügung gestellt wird, ist sofort weltweit nutzbar.

Die Megamaschine und damit eine nivellierend wirkende Infrastruktur trifft aber auf eine uneinheitliche, *noch nicht vorbereitete Welt*, denn sie verbindet Staaten aller gesellschaftspolitischen Formen, egal ob es sich um Demokratien unterschiedlicher Prägung, Diktaturen oder die verbleibenden sozialistischen Volksrepubliken handelt. Sie verbindet demzufolge auch Staaten, die Konflikte miteinander austragen, und läßt unterschiedliche Wertesysteme aufeinanderprallen.

Daraus ergeben sich Chancen und Risiken für eine demokratische Entwicklung von Staaten und die Sicherheit und das Wohlbefinden der in ihnen lebenden Menschen. Wesentliche Faktoren dabei sind die ungehindert Grenzen überschreitende Kommunikation, die demokratische Ideen ebenso verbreiten kann wie deren Gegenteil, die „Demokratisierung" der Computernutzung, die sich daraus ergibt, daß Computerressourcen unabhängig von ihrem Standort überall und zu jeder Zeit zur Verfügung gestellt werden können – und somit für rechtschaffene Zwecke und für deren Gegenteil bereitstehen, sowie die Angriffspotentiale, die von jedem Punkt der Welt aus über das Netz wirken können, um Datenkommunikation zu unterbinden, zu manipulieren, abzuhören, unzuverlässig zu machen, Informationen anzubieten, die die Wertesysteme anderer ins Wanken bringen sollen. Zugleich droht eine weltweite Spaltung in „informationsreiche" und

„informationsarme" Länder und Bevölkerungsgruppen.

Überall bemühen sich Teilnehmer im Internet, das Netz ihren Zielen entsprechend zu nutzen, die durchaus im direkten Gegensatz zu den Zielen anderer stehen können. Es finden nicht nur bereitwillige Kommunikation und Informationsbereitstellung statt, sondern auch Angriffe auf die Sicherheit anderer Teilnehmer.[36]

Durchaus riskant in dieser Hinsicht sind Neuentwicklungen im Internet, die neben den zweifellos hilfreichen Aspekten auch erhebliche Sicherheitsaspekte aufwerfen. Zunehmend werden Techniken entwickelt, die bewirken, daß beim Aufruf von Internet-Diensten – etwa dem World Wide Web (WWW) – Programme vom Anbieter in das System des Nutzers übertragen werden. Die Programmiersprache „*Java*" ist speziell dafür entwickelt, die sog. „*Cookies*" dienen dazu, dem Anbieter Informationen über den Nutzer zu übermitteln, die diesen von Routineangaben entlasten – beides Techniken, die auch bösartige Effekte hervorrufen können[37].

Risiken aus Neuentwicklungen werden erkannt, Mailinglisten der CERT's, einschlägige Newsgruppen und die Fachpublikationen werden ausgewertet. Speziell zu Cookies, Java und Javascript wurde vom Landesamt für Informationstechnik gegenüber Anwendern auf den Verzicht dieser Browseroptionen hingewiesen. Solche und ähnliche Richtlinien, wie z.B. auch für die Abwendung von Computerviren, werden in der vom Landesamt für Informationstechnik 1997 zu erstellenden Verwaltungsrichtlinie Telekommunikation zusammengefaßt werden.

Internetnutzung der Berliner Verwaltung

Für die öffentliche Verwaltung Berlins bedeutet die Anbindung an offene Netze, daß sie Bürger, Klienten, Kunden besser mit Informationen versorgen, also Transparenz bewirken kann, und daß sie Dienstleistungen anbieten kann, die über die reine Informationsbereitstellung hinausgehen. Damit können Ziele der Verwaltungsreform wie Bürgernähe und rationelle, schnelle Bearbeitung von Routinevorgängen erreicht werden.

Die Senatsverwaltung für Inneres hat sowohl in dem bereits erwähnten Rahmenkonzept als auch in detaillierten Rundschreiben zur „Nutzung des Internet" die technisch-organisatorischen Mindestanforderungen an eine Nutzung des Internets für Verwaltungsaufgaben festgelegt. Diese Anforderungen stimmen weitestgehend mit entsprechenden Empfehlungen des Berliner Datenschutzbeauftragten überein.

Die Anbindung an offene Netze bedeutet aber auch die Konfrontation mit den Sicherheitsproblemen. Das Problem ist also: Wie können die Dienstleistungen der öffentlichen Verwaltung möglichst ohne Einschränkung über das Internet an den Bürger gebracht werden, ohne daß andererseits die Angriffspotentiale die Dienstleistungen in vielfältiger Weise gefährden? Mit den diesbezüglichen Bemühungen der Berliner Verwaltung befassen wir uns unten.[38]

Werden die im Internet verfügbaren Programme und Datenformate zur Erschließung, Bereitstellung, Strukturierung und Präsentation von Informationen in unternehmens- oder verwaltungsinternen Netzen an, so wird von Intranets gesprochen. Damit wird es möglich, organisationsweit Informationen bereitzustellen, die beliebig miteinander verknüpft werden können.

Auch die Berliner Verwaltung bietet ihren an das Berliner Landesnetz angeschlossenen Behörden und deren Mitarbeitern ein *Intranet* angewendet, um interne Informationen effizienter verbreiten zu können. Solange es sich hierbei um allgemeine Informationen über die Verwaltung handelt oder regelnde Informationen verwaltungsweit verbreitet werden sollen, ist aus datenschutzrechtlicher Sicht dazu nichts zu sagen, solange keine Sicherheitslücken in der Informationstechnik (IT) damit aufgerissen werden. Jedoch wird eine gefährliche Tendenz verstärkt, die grundsätzlich mit einer verwaltungsübergreifenden offenen Vernetzung verbunden ist: Die verfassungsrechtlich gebotene Abschottung der Informationskanäle zwischen Behörden unterschiedlicher Aufgaben bei der Verarbeitung personenbezogener Daten (*informationelle Gewaltenteilung*) wird weiter in Frage gestellt, wenn immer mehr und leistungsfähigere Instrumente zur behördenübergreifenden Kommunikation bereitgestellt werden.

Die Forderung nach der informationellen Gewaltenteilung wird durch die Sicherheitsrahmenrichtlinie der Senatsverwaltung für Inneres in Form der verfahrens- und behördenbezogenen Sicherheitsdomänen gefaßt. Die behördenübergreifende Kommunikation zwischen den verschiedenen Sicherheitsdomänen wird durch Sicherheitsdienstleistungen des Landesamtes für Informationstechnik im Bereich der Backbone- und Grenznetzdienste nach diesen Grundsätzen gestaltet. Dazu werden zwischen dem Landesamt für Informationstechnik und den IT-Anwendern eine Rahmenregelung und Serviceleistungen (Servicescheine) vereinbart.

[36] vgl. unten 4.8.2
[37] vgl. unten 4.8.4
[38] vgl. unten 4.8.2

Chipkarten

Nur scheinbar unabhängig von der Herausbildung der Megamaschine Internet ist die zunehmende Verbreitung von Chipkarten. Diese am meisten miniaturisierte Form informationstechnischer Systeme hat im letzten Jahr weitere Verbreitung gefunden, allerdings augenscheinlich noch weniger in den Taschen der Bürger, Kunden und Klienten als vielmehr als Pilotprojekte in vielen verschiedenen Lebenszusammenhängen.

Chipkarten sind miniaturisierte IT-Komponenten, meist in der genormten Größe einer Kreditkarte. Auch wenn die Zahl der Anwendungen, die bereits in den Routinebetrieb gegangen sind, noch relativ klein ist, so werden sie dennoch zunehmend an gesellschaftlicher Bedeutung gewinnen.

Die derzeit bekannteste Chipkarten-Anwendung ist die *Telefonkarte*, die ein Guthaben enthält, das beim Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird. Es ist ganz offensichtlich, daß eine solche anonyme Anwendung von Chipkarten aus datenschutzrechtlicher Sicht Vorbildcharakter hat.

Ebenfalls allgemein verbreitet ist die *Krankenversichertenkarte*, die lediglich einen gesetzlich vorgegebenen Inhalt hat und zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Sie ist ein Beispiel für eine Chipkarte, die lediglich die dem Versicherten erkennbare Oberfläche einer umfassenden IT-Infrastruktur ist. Was unterhalb dieser Oberfläche geschieht, ist für die Betroffenen nicht transparent. Damit ist sie auch ein erstes Beispiel für die Zusammenhänge zwischen Chipkarten und vernetzten Systemen, insbesondere auch dem Internet. In diesem Falle geht es um die Weiterverarbeitung, vor allem auch den Weitertransport der auf der Chipkarte gespeicherten Daten.

Weitere neue Anwendungsbereiche sind derzeit in der Diskussion bzw. in der Erprobung, z.B. die Chipkarte im bargeldlosen Zahlungsverkehr als elektronische Geldbörse sowie Gesundheits- oder Patientenchipkarten zur Speicherung und Übermittlung medizinischer Daten.

Technisch kann man diese reinen Speicherchipkarten zur Aufnahme von Daten von solchen Karten unterscheiden, die zusätzlich Mikroprozessoren enthalten. Solche Prozessorchipkarten sind Kleinstcomputer, denen nur die Möglichkeit zur Kommunikation zwischen Mensch und System fehlt. Ihre Verwendung bedarf also zusätzlicher technischer Systeme zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren und zum Beschreiben der Speicher

Derartige Chipkartensysteme gibt es bereits in vielen verschiedenen Ausprägungen, z.B.:

- Öffentliches Telefon-Kartenterminal
- Funktelefon (Handy)
- PC mit externem Kartenterminal oder integriertem Kartenleser
- Laptop mit Chipkarten-Leser
- Geldausgabeautomat
- Point-of-Sale-Kartenterminal (POS-Kartenterminal)
- Versicherten-Kartenterminal in seiner Stand-alone-Ausführung (ohne PC-Anschluß)
- Kontoauszugsdrucker
- Airline-Check-in-Terminal
- Customer-Service-Terminal
- Fahrschein-/Parkticket-Terminal
- AsylCard[39]

[39] vgl. unten 4.2

Chipkarten werden in diesen Systemen in unterschiedlicher Weise gebraucht:

Sie sind Speicher von Daten, deren Vertraulichkeit und/oder Integrität hohen Schutz erfordern (z.B. Kontodaten, medizinische Individualdaten, Personalausweisdaten, Führerscheindaten). In diesem Falle werden die Daten gespeichert, um sie bei Bedarf in andere Systeme, in der Regel auch über umfangreiche Netze, zur weiteren Verarbeitung zu übertragen. Die Daten müssen nicht immer wieder beim Inhaber erfragt (unter Umständen mit unterschiedlichen Angaben) und per Hand erfaßt werden.

Chipkarten sind Träger elektronischen Geldes. Die Telefonkarte stellt hier ein sehr einfaches Beispiel dar. Sie kann nicht wieder aufgefüllt werden. Elektronische Geldbörsen werden sich dagegen wieder aufladen lassen und in unterschiedlichsten Situationen eingesetzt werden können. Sie bieten die Chance zur anonymen, zumindest pseudonymen Zahlweise.

Chipkarten sind aber auch Mittel zur Authentisierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten). Hierfür speichern sie die Codes, die den Zugriff auf entfernte Datenbestände ermöglichen. Damit verwandt ist ihre Funktion als Mittel zur *Signatur von Dokumenten* (Verträge, Willenserklärungen, Befunde etc.), weil nur sie geeignet sind, die dafür erforderlichen langen Schlüssel mit dem notwendigen Schutz gegen unbefugte Nutzung zu speichern und bei Bedarf zu übertragen. Chipkarten bieten vor allem als Authentisierungsinstrumente erhebliche Chancen für die sichere Nutzung von Informationssystemen. Sie sind geeignet, Individualdaten sicher vor unbefugten Zugriffen zu bewahren, bis sie benötigt werden.

Allerdings wirft ihr Gebrauch erhebliche datenschutzrechtliche Probleme auf:

Der Umstand, daß der Inhaber der Chipkarte große Mengen an sensiblen Individualdaten bei sich trägt sowie mit den Authentifizierungsmöglichkeiten der Chipkarte erschließen kann, kann große Begehrlichkeiten erwecken. Hier liegen z.B. die Gefahren der Gesundheitschipkarten, die Krankengeschichten enthalten oder erschließen. In vielen Fällen ist einsichtig, daß die Bereitstellung solcher Daten für den Patienten von Nutzen sein können. Sie kann sich aber auch gegen ihn richten, wenn die Zweckbindung nicht beachtet wird.

Die große Bedeutung von Chipkarten für die informationstechnische Sicherheit stellt die Frage nach der Sicherheit der Chipkarte selbst. Kann sie manipuliert, unzulässigerweise ausgelesen oder sonstwie genutzt werden, so verkehrt sich ihre Sicherheitswirkung für andere Systeme ins Gegenteil.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten" ausgearbeitet.

In Berlin verläuft der Einsatz der neuen Technologie eher zögerlich:

Die Berliner Verkehrsbetriebe (BVG) haben ein Pilotprojekt für die Nutzung einer wiederaufladbaren, anonymen, elektronischen Geldbörse auf einigen Buslinien durchgeführt. Dieses Projekt, dem wir wegen der Sicherstellung der Anonymität zugestimmt hatten, ist jedoch inzwischen eingestellt worden.[40]. Inzwischen ist ein neues Projekt zur Einführung einer elektronischen Geldbörse geplant, die dann jedoch auch für andere Zwecke, etwa Museumsbesuche, genutzt werden kann

Der hier vom Berliner Datenschutzbeauftragten erweckte Eindruck, Chipkarten würden zur Speicherung von Führerscheindaten verwendet, ist unzutreffend. Darüber hinaus besteht auch nicht die Absicht, in der Bundesrepublik die Speicherung von Führerscheindaten auf Chipkarten einzuführen. Der Scheckkartenführerschein, der im Zuge der Umsetzung der 2. EU-Führerscheinrichtlinie in nationales Recht gegen Mitte 1998 eingeführt werden soll, wird nach derzeitiger Kenntnis nicht mit einem Chip ausgestattet sein.

[40] JB 1993, 2.3.

(BerlinCard).

Das Projekt „Berliner Gesundheitspaß", mit dem geplant war, interessierten Berliner Bürgern eine umfassende Krankengeschichte auf der Chipkarte in die Hand zu geben, um auch die Eigenverantwortlichkeit der Patienten zu fördern, wurde mit dem Wechsel an der politischen Spitze der Gesundheitsverwaltung eingestellt[41].

Es bestehen Pläne (z.B. in der Humboldt-Universität) zum Einsatz multifunktionaler Chipkarten im Universitätsbereich (UniversCard), mit denen u.a. Funktionen der Universitätsverwaltung, der Zugangskontrolle zu Räumlichkeiten und Geräten, beim Hochschulwechsel sowie der bargeldlosen Zahlung in Mensen und Bibliotheken ausgeführt werden können.

2.2 Datenschutz durch Technik

Die Informationstechnik wird heute nicht mehr nur als etwas angesehen, was Risiken für die informationelle Selbstbestimmung der Menschen heraufbeschwört und was durch zusätzliche organisatorische und technische Maßnahmen so zu gestalten ist, daß Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Ressourcen gewährleistet werden können. Es ist inzwischen erkannt, daß technische Verfahren und Methoden dazu dienen können, Datenschutz und Sicherheit zu produzieren. Datenschutz durch Technik und nicht Datenschutz trotz Technik sollte das Ziel sein. Es war zwar schon immer bekannt, daß die Automation stets neue Sicherheitsprobleme aufwarf, auf deren Lösung mit technisch-organisatorischen Mitteln die Datenschutzbeauftragten bestanden. Gleichzeitig konnten mit der Automation aber auch erstmals Probleme der Sicherheit gelöst werden, die bei den nicht-automatisierten Verfahren nicht beherrschbar waren.

So ermöglicht die moderne Informationstechnik den Einsatz komplizierter, aber dafür um so leistungsfähigerer kryptographischer Verfahren, so daß Vertraulichkeit auf einem Niveau erreicht werden kann, das in der nicht-automatisierten Datenverarbeitung und mit der Informationstechnik früherer Jahre nicht annähernd erreicht werden konnte[42].

Datenschutz durch Technik weist den Weg aus drei Alternativen: Nimmt man Risiken in Kauf und lernt mit ihnen und mit den konsequenterweise eintretenden Verletzungen der informationellen Selbstbestimmung zu leben, wie von computer- und netzversessenen Zeitgenossen nicht selten erwartet wird? Oder stellt man die maschinenstürmerische Forderung nach einer Eingrenzung der Informationstechnologie zur Debatte? Oder versucht man, die Probleme mit denselben Mitteln zu lösen, mit denen sie heraufbeschworen wurden? Es ist klar, daß nur der dritte Weg in Frage kommt.

Jeder Nutzer hinterläßt immer mehr elektronische Spuren bei der Nutzung der Informationstechnik. Damit können komplexe Persönlichkeitsprofile über ihn zusammengestellt und mißbraucht werden, ohne daß er dies kontrollieren könnte, denn über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck dieser Daten kann er keine Kontrolle mehr ausüben.

Dieser Gefahr kann begegnet werden, indem die Frage nach der Erforderlichkeit personenbezogener Daten vermehrt gestellt wird und Datensparsamkeit bis hin zur Datenvermeidung angestrebt wird. Durch die Nutzung neuer Möglichkeiten der modernen Informationstechnik ist es in vielen Anwendungsfällen möglich, die Verarbeitung personenbezogener Daten vollständig

[41] JB 1995, 3.2.
[42] vgl. unten 3.4

auszuschließen. Datensparsamkeit und Datenvermeidung werden sich zunehmend als Wettbewerbsvorteil erweisen.

Während bei der rechtlichen Bewertung strenge Erforderlichkeitsanforderungen gestellt werden, nimmt man es mit der Erforderlichkeit personenbezogener Daten in informationstechnischen Systemen nicht so genau. Dabei geht es allerdings nicht primär um das Auftreten dieser Daten überhaupt, sondern um die Identifizierbarkeit der Personen, deren Daten in Informationssystemen auftreten.

Die Identität der Personen, deren Daten verarbeitet werden, ist für die meisten Verarbeitungsschritte unerheblich. Vielmehr gibt es eine Vielzahl von Verfahren, die völlig ohne die Identität des Betroffenen auskommen, die also mit *anonymen* Daten arbeiten können. In anderen Verfahren muß die Identität nur in besonderen Ausnahmefällen und dann nur außerhalb des technischen Systems festgestellt werden. Solche Systeme können dann ausschließlich mit *Pseudonymen* arbeiten. In vielen Verfahren ist die Identifikation des Einzelnen nur in Teilprozessen erforderlich, in anderen jedoch nicht. Das System kann dann also in bestimmten Domänen Pseudonyme aufdecken, in anderen nicht. Schließlich bleiben die Verfahren, in denen die Identifizierbarkeit überall erforderlich ist.

Bei modernen Client-Server-Systemen kann man davon ausgehen, daß selbst in allen Systemen, in denen die Identifizierbarkeit der Betroffenen eine wichtige Rolle spielt (z.B. polizeiliche Fahndungssysteme, Abrechnungs- und Zahlungssysteme, Melderegister, Patientendatensysteme), die Identität der Personen erst an den Mensch-Maschine-Schnittstellen gelüftet werden muß, an denen Entscheidungen zu den Individuen gefällt und Handlungen für oder gegen die Personen veranlaßt werden. Es reicht dann, wenn das System fast überall mit Pseudonymen arbeitet und nur der Rechner des für die Bearbeitung oder sonstige Nutzung zuständigen Mitarbeiters die Identität wiederherstellen kann.

Bei anonymen Zahlungsverfahren, z.B. bei Zahlungen mit vorausbezahlten Guthaben auf der Chipkarte, genügt stets die Arbeit mit Pseudonymen. Hier muß nur im Einzelfall, also bei einer Reklamation, nachvollzogen werden können, wer der Inhaber der Karte eigentlich ist. In diesen Fällen wäre es dann der Inhaber, der das Pseudonym lüftet. Denkbar wäre auch die Einschaltung neutraler dritter Stellen (Trusted Third Parties). Völlig anonym ist die Nutzung der Telefonkarte mit vorausbezahltem Guthaben. Hier kann das Nutzerverhalten bei der Telefonkommunikation selbst dann nicht nachvollzogen werden, wenn ein sich identifizierender Kunde sich über eine von ihm vorgelegte Karte beschwert.

Dieser Ansatz ist unter dem Begriff „Privacy-enhancing Technologies – PET" (Datenschutz-freundliche Technologien) von der Registratiekamer der Niederlande (Holländischer Datenschutzbeauftragter) und dem Privacy Commissioner for the Province of Ontario, Canada, in die internationale Datenschutzdiskussion eingebracht worden[43]. Er geht davon aus, daß viele datenschutzrechtliche Probleme gelöst oder gemildert werden können, wenn die Identität der Betroffenen durch kryptographische Methoden pseudonymisiert wird, solange dies nicht im Widerspruch zu den Anwendungszielen steht. Er geht weiter davon aus, daß ein solcher Widerspruch nur in wenigen Bereichen eines Informationssystems besteht.

Die dringend erforderliche Anpassung der zehn Forderungen der Datenschutzgesetze zu technisch-organisatorischen Maß-

In dem auch im Bericht positiv erwähnten Rahmenkonzept zur IT-Sicherheit (vgl. Ziffer 4.8.2) wird dieser Gedanke

[43] Registratiekamer of The Netherlands, Information and Privacy Commissioner of Ontario, Canada: Privacy-enhancing Technologies – The path to anonymity, Vol. I und II , Rijswijk, 1995

nahmen (Anlage zu § 9 BDSG) an moderne, künftig global vernetzte informationstechnische Infrastrukturen könnte hier einen Ansatz finden. Viele Schutzanforderungen relativieren sich und können billiger realisiert werden, wenn mit der Anonymisierung bzw. Pseudonymisierung der Schutzbedarf der Daten herabgesetzt wird. Dies entspricht dem Gedanken, daß die Sicherheit der Datenverarbeitung aus der sinnvollen Kombination von einander ergänzenden Maßnahmen, nicht jedoch aus der Summe teurer Einzelmaßnahmen entsteht.

Bei bestimmten Dienstleistungen wie der Wartung, Fernwartung oder Administration ist der Zugriff auf personenbezogene Daten nie erforderlich, derzeit häufig aber nicht vermeidbar. Die Vorbehalte gegen solche Leistungen, die zunehmend von Fremdpersonal erbracht werden, ließen sich mit datenschutzfreundlicher IT zurücknehmen.

Für die Überwachung des ökonomischen, sicheren, ordnungsgemäßen und datenschutzgerechten Betriebs eines IT-Systems kommt man ohne Protokollierung nicht aus. Die Protokolle erzeugen ihrerseits wieder Risiken für die informationelle Selbstbestimmung der Betroffenen (deren Daten als Objekte des überwachten Datenverarbeitungsprozesses in die Protokolle eingehen) und der Benutzer (deren Handeln protokolliert wird). Datenschutzfreundliche IT hilft hier, denn für die Routinekontrolle reichen die Pseudonyme in beiden Rollen. Eine Re-Pseudonymisierung wäre nur in regelbaren und einer besonderen Kontrolle unterworfenen Einzelfällen nötig.

Die Abrechnung von Dienstleistungen, die elektronisch gemessen, abgerechnet und zahlbar gemacht werden können, wie z.B. die Nutzung informations- und kommunikationstechnischer Dienste, soll die tatsächliche Inanspruchnahme der Dienste berücksichtigen. In vielen Fällen läßt sich dies völlig anonym gestalten. Bei Reklamationen sind jedoch Aufzeichnungen notwendig, die die Inanspruchnahme nachweisen. Diese Aufzeichnungen ermöglichen dann die „gläsernen Verbraucher" oder stehen dem Grundrecht auf „unbeobachtete Kommunikation" entgegen. Auch diese Aufzeichnungen könnten pseudonym geschehen.

Sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft sollten künftig „Privacy enhancing Technologies" einen hohen Stellenwert einnehmen.

explizit aufgegriffen und als zu beachtende Anforderung bei der Verfahrensentwicklung formuliert.

Für die Gewährung vereinbarter Zugriffsrechte und zur Leistungsabrechnung werden im Bereich der netzbezogenen Sicherheitsdienstleistungen des Landesamtes für Informationstechnik anonymisierte Zugangsformen vorgesehen. Hinter einer mnemonischen Kennung verbirgt sich in der Regel eine ausreichend große Anzahl von gleichberechtigten Anwendern.

3. Schwerpunkte im Berichtsjahr

3.1 Erkennungsdienstliche Behandlung

Zwei Vorgänge im vergangenen Jahr lenkten die Aufmerksamkeit wieder einmal auf die Problematik der erkennungsdienstlichen Behandlung durch die Polizei: Schon früher hatten wir über Fälle der Überreaktion berichtet[44].

Diesmal erhielten wir mehrere Beschwerden von Bürgern, die im Bereich des Bahnhofes Zoologischer Garten oder des Breitscheidplatzes im Rahmen einer Razzia überprüft und – auch wenn sie ihre Identität nachweisen konnten – erkennungsdienstlich behandelt wurden. Mit der Begründung, das Gelände rund um den Bahnhof Zoologischer Garten sei ein bevorzugter Treffpunkt von Stadtstreichern, Trebegängern, Personen aus dem Drogenmilieu, Personen, die der Prostitution nachgehen, sowie deren Freiern, Angehörigen anderer Randgruppen, einer Vielzahl von Ausländern, oft im Kindesalter und ohne Aufenthaltsgenehmigung, hat die Polizei das Gebiet, ebenso wie den Breitscheidplatz, als *„gefährlichen Ort"* eingeordnet (§ 21

Der Berliner Datenschutzbeauftragte erweckt im folgenden mit seinen Behauptungen, im Zusammenhang mit erkennungsdienstlichen Behandlungen habe es Überreaktionen der Polizei gegeben, die Polizei könne auf keinen Fall beliebig erkennungsdienstliche Maßnahmen vornehmen und es könne der Verdacht entstehen, daß Ziel der Maßnahme die Abschreckung der Betroffenen sein solle den Eindruck, es sei gängige Praxis der Polizei, rechtswidrig erkennungsdienstliche Maßnahmen mit dem Ziel der Einschüchterung vorzunehmen.

Eine derartige Bewertung ist aus den tatsächlichen Geschehen nicht abzuleiten. Es geht nicht an, daß ein Einzelfall, bei dem

[44] JB 1990, 3.5, JB 1991, 3.4.1

Allgemeines Sicherheits- und Ordnungsgesetz – ASOG –). Um einer Verfestigung dieser Strukturen entgegenzuwirken, werden von der Polizei in diesem Bereich Schwerpunkteinsätze durchgeführt. Dabei werden einzelne Personen und Personengruppen überprüft und einer Identitätsfeststellung unterzogen. In Einzelfällen wird eine Abfrage im Polizeicomputer über Funk veranlaßt. Ergibt sich, daß gegen den Betroffenen einmal ein Ermittlungsverfahren geführt wurde oder aktuell geführt wird, werden vor Ort Lichtbilder der Person angefertigt. In der Praxis führte das dazu, daß die Polizei sich bei einzelnen Bürgern entschuldigen mußte.

Das NDR-Magazin „Panorama" berichtete aufgrund von Aussagen eines pensionierten Berliner Polizeibeamten, daß jahrelang *rumänische Abschiebehäftlinge* durch die Berliner Polizei in unwürdiger Weise erkennungsdienstlich behandelt worden seien und das daraus gewonnene Bildmaterial in die Lichtbildkartei eingestellt worden sei. Eine datenschutzrechtliche Prüfung des Vorganges hat ergeben, daß sich unter 102 stichprobenhaft nach Staatsangehörigkeit ausgewählten Fällen 25 Fälle in der Lichtbildkartei befanden, bei denen Personen in einer Weise abgebildet waren, die den erhobenen Vorwürfen entsprachen. Die Personen, die mit polizeieigenen Trainingsanzügen ohne Reißverschluß abgelichtet wurden, waren durchgängig zu inakzeptablen Haltungen gezwungen: sie stellten sich mit entblößter Brust dar, in einem Fall trug auch eine Frau ein vorn offenes Oberteil ohne Unterwäsche. Einige Betroffene hatten zerrissene Stoffteile vor der Brust verknotet. In einem Fall waren unter der weit geöffneten Jacke Verletzungen erkennbar.

die Polizei selbst noch am Tage der Anfertigung von Lichtbildern diese wieder vernichtet hat, als Anlaß dafür herhalten muß, der Polizei ein mangelndes Datenschutzbewußtsein vorzuhalten. Der Umstand, daß die Polizei die aufgrund einer falschen rechtlichen Bewertung zunächst angefertigten Lichtbilder noch am selben Tage von sich aus wieder vernichtet hat, zeigt, daß behördeninterne Kontrollmechanismen funktionieren. Die rechtliche Fehleinschätzung der vor Ort eingesetzten Beamten wurde noch am gleichen Tage korrigiert, ohne daß es eines Anstoßes bzw. der Beanstandung durch den Datenschutzbeauftragten bedurft hätte.

Die vom Datenschutzbeauftragten bezeichneten Fälle stammen aus den Jahren 1990 bis 1994. Bereits der damalige für die Aufsicht über die Polizei zuständige Staatssekretär in der Innenverwaltung hatte am 5. August 1994 die Polizeibehörde angewiesen, auf eine Änderung der Verhältnisse hinzuwirken. Sie hatte wiederum den Gesamtvorgang zum Anlaß genommen, die verantwortlichen Bereiche darauf hinzuweisen, daß auch unter dem notwendigen Aspekt der Sicherheit auf ein zumutbares Erscheinungsbild zu achten sei. Seit August 1994 sind keine weiteren Vorwürfe bekannt geworden.

Es steht außer Zweifel, daß die angefertigten Bilder bedrükken. Der Senator für Inneres hat sowohl gegenüber dem Abgeordnetenhaus als auch gegenüber seinem Ausschuß für Inneres, Sicherheit und Ordnung sein Bedauern darüber zum Ausdruck gebracht, daß es in der Vergangenheit zu einer Bekleidung rumänischer Tatverdächtiger mit beschädigter und teilweise unvollständiger polizeilich gestellter Bekleidung gekommen ist.

In der Sitzung des Unterausschusses Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung im Dezember 1996 wurde hierzu erklärt, daß die Lichtbildsammlung sukzessive auf das nicht auszuschließende Vorhandensein weiterer derartiger Bilder durchgesehen und dann eine Entfernung vorgenommen wird. Eine komplette Durchsicht dieser Sammlung im Rahmen einer Sonderaktion ist angesichts deren Umfangs (ca. 184 000 Bilder) personell gegenwärtig jedoch nicht leistbar. Hierüber wurde Einvernehmen mit dem Datenschutzbeauftragten erzielt. Der Aufbau einer elektronischen Lichtbildsammlung in diesem Jahr wird dazu genutzt werden, bei der Übernahme des bisherigen Gesamtbestandes die jeweilige Rechtmäßigkeit und Aufbewahrungsnotwendigkeit zu überprüfen. Schon jetzt ist sichergestellt, daß bei weiterem Erkennen derartige Bilder vernichtet werden.

Zulässige Maßnahmen

Regelungen für die Durchführung *erkennungsdienstlicher Maßnahmen* sind in den *Polizeigesetzen* der Länder und in der *Strafprozeßordnung* enthalten. Hierzu zählen die Abnahme von Finger- und Handflächenabdrücken, die Aufnahme von Lichtbildern, Messungen und die Feststellung anderer äußerlicher, körperlicher Merkmale (§ 23 Abs. 3 ASOG, § 81 b StPO). Im Gegensatz zu anderen Ländern, in deren Polizeigesetzen die Maßnahmen abschließend aufgeführt sind, ist der Katalog von erkennungsdienstlichen Maßnahmen im Berliner ASOG nicht abschließend. Es werden auch ähnliche Maßnahmen zugelassen, soweit sie keinen stärkeren Eingriff in Grundrechte des Betroffenen darstellen. Denkbar sind hier die Fixierung des Klanges einer Stimme auf einem Tonträger sowie Schriftproben. Das ASOG beschränkt diese Methoden auf die Feststellung äußerlich wahrnehmbarer Merkmale, die nicht mit Eingriffen in die körperliche Unversehrtheit verbunden sind

Hierzu hält der Senat eine Stellungnahme nicht für geboten. Der Datenschutzbeauftragte erklärt selbst, daß die Sinnhaftigkeit von polizeilichen Datensammlungen nicht aus datenschutzrechtlicher, sondern aus kriminalistischer Sicht zu beurteilen ist.

(§ 23 Abs. 3 Nr. 3 ASOG). Auf dieser Grundlage bewahrt die Polizei offenbar auch recht eigenwillige Bestände auf, wie die Ohrenabdruckspuren-Sammlung, die sie von der ehemaligen Volkspolizei der DDR übernommen hat[45]. Inwieweit diese Datensammlung tatsächlich sinnvoll für die Straftatenaufklärung genutzt werden kann, ist fraglich – aber nicht aus datenschutzrechtlicher, sondern aus kriminalistischer Sicht zu beurteilen. Zu den erkennungsdienstlichen Maßnahmen gehören nicht Genomanalysen, die nur als Beweismittel im Strafverfahren eingesetzt werden[46].

Identitätsfeststellung

Die Polizei kann erkennungsdienstliche Maßnahmen vornehmen, wenn eine *Identitätsfeststellung* auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist (§ 23 Abs. 1 Nr. 1 ASOG). Voraussetzung ist, daß die Identitätsfeststellung selbst zulässig ist. Das ist der Fall, wenn es zur Abwehr einer im Einzelfall bestehenden (konkreten) Gefahr oder zur Erfüllung der der Polizei durch andere Rechtsvorschriften zugewiesenen Aufgaben erforderlich ist (§ 21 Abs. 1 ASOG).

Ohne daß ein konkreter Verdacht gegen die zu überprüfende Person vorliegen muß, kann die Polizei bei *Razzien* an „gefährlichen Orten" die Identität der angetroffenen Personen feststellen. Das sind Orte, an denen Straftaten von erheblicher Bedeutung verabredet, vorbereitet oder verübt werden oder an denen sich Personen treffen, die gegen aufenthaltsrechtliche Vorschriften verstoßen, und Orte, an denen sich gesuchte Straftäter verbergen oder an denen der Prostitution nachgegangen wird.

Nur wenn die Identität des Betroffenen nicht anders festgestellt werden kann, d.h. er sich nicht ausweisen kann und auch nicht durch andere Unterlagen seine Identität feststellbar ist, darf die Polizei Personen, die sie bei einer Razzia überprüft, einer erkennungsdienstlichen Maßnahme unterziehen. Hier ist jedoch der Verhältnismäßigkeitsgrundsatz zu beachten. Auch an „gefährlichen Orten" darf die Polizei nicht wahllos Personen kontrollieren. Es müssen Tatsachen ersichtlich sein, daß die Person mit den Besonderheiten des Ortes in einem Zusammenhang steht. Auch wenn der Anlaß der Überprüfung nur geringfügig ist und keine Anhaltspunkte dafür vorliegen, daß der Betroffene eine falsche Auskunft gegeben hat, muß die Polizei die noch bestehende Ungewißheit über dessen Identität hinnehmen.

Ist die Identität festgestellt, sind die angefallenen erkennungsdienstlichen Unterlagen grundsätzlich zu *vernichten*. Eine weitere Aufbewahrung ist nur zulässig, wenn es zur vorbeugenden Straftatenbekämpfung erforderlich ist oder andere Rechtsvorschriften es zulassen, z.B. § 81 b StPO, wenn der Betroffene einer Straftat verdächtig ist.

Die Möglichkeit der Identitätsprüfung an „gefährlichen Orten" wurde in den Anhörungen zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes kritisiert, da diese Maßnahmen nicht an ein polizeirechtsrelevantes Verhalten oder einen Tatverdacht geknüpft werden, sondern allein die Anwesenheit an einem als gefährlich deklarierten Ort ausreicht.

Im *Ausländerbereich* ist zu beobachten, daß sich das Instrument der erkennungsdienstlichen Behandlung von dem ursprünglichen Zweck – der Identitätsüberprüfung – zu einem ausländerrechtlichen Fahndungsinstrument entwickelt hat. Knüpft das Allgemeine Sicherheits- und Ordnungsgesetz noch an das polizeirechtliche Merkmal des „gefährlichen Ortes" an,

Der Senat verweist auf seine Stellungnahme zu 3.1 (Erkennungsdienstliche Behandlung).

Natürlich darf die Polizei nicht wahllos Personen kontrollieren. Der Senat hat jedoch keine Anhaltspunkte dafür, daß die Polizei so verfährt.

Bei dem kritisierten § 16 Asylverfahrensgesetz handelt es sich um eine bundesrechtliche Vorschrift, die durch die Gesetzesnovellierung im Rahmen des sogenannten Asylkompromisses 1992 neu gefaßt wurde. Ob sich der Bundesgesetzgeber mit der Neufassung des Asylverfahrensgesetzes verfassungskonform verhalten hat, entscheidet allein das Bundesverfassungsgericht.

[45] JB 1991, 2.2
[46] vgl. unten 4.3.1

ist bei *Asylbewerbern* jegliche eingrenzende Voraussetzung für die Durchführung einer erkennungsdienstlichen Behandlung entfallen. Allein die Tatsache, daß es sich um einen Ausländer handelt, der Asyl begehrt, ist ausreichender Anlaß für eine erkennungsdienstliche Behandlung (§ 16 Abs. 1 Asylverfahrensgesetz). Die ursprünglich auch für Asylbewerber geltende Regelung, daß eine erkennungsdienstliche Behandlung nur gerechtfertigt ist, wenn die Identität des Betroffenen nicht eindeutig bekannt ist, wurde mit dieser Bestimmung aus dem Jahr 1992 abgeschafft.

Die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* hat sich 1992 mehrheitlich gegen die ausnahmslose Erfassung gewandt, da dies mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren ist[47]. Die erkennungsdienstliche Behandlung von Ausländern, die um Asyl nachsuchen – auch wenn deren Identität feststeht -, sowie die nahezu unbeschränkte Nutzung der Unterlagen für Zwecke der Strafverfolgung (§ 16 Abs. 5 Asylverfahrensgesetz) sind mit dem Menschenbild des Grundgesetzes und der Europäischen Menschenrechtskonvention kaum vereinbar.

Ein entsprechender Vorstoß wurde etwa zwei Jahre später in Berlin für *Bürgerkriegsflüchtlinge* mit bosnischen Identitätspapieren unternommen. Nachdem – ähnlich wie damals bei den Asylbewerbern – die erkennungsdienstliche Behandlung zunächst auf bestimmte Volksgruppen beschränkt werden sollte, bei denen Identitätstäuschungen häufiger vorkommen, soll jetzt durch Änderung des Ausländergesetzes eine generelle erkennungsdienstliche Behandlung durchgesetzt werden. Waren es bei den Asylbewerbern zunächst Menschen aus Ghana, dem Senegal, dem Libanon und Palästinenser[48] sollten später Bürgerkriegsflüchtlinge mit bosnischen Identitätspapieren[49] generell erkennungsdienstlich behandelt werden. Bei den Bürgerkriegsflüchtlingen hat die Senatsverwaltung für Inneres von dieser Maßnahme abgesehen, allerdings nicht wegen der von uns geäußerten rechtlichen Bedenken[50], sondern aus Kapazitätsgründen[51].

Das Abgeordnetenhaus hat dennoch im November 1996 als „*Maßnahme gegen den Leistungsmißbrauch*" den Senat aufgefordert, in den Bundesrat eine Vorlage zur Änderung des Ausländergesetzes einzubringen[52]. Beabsichtigt ist, § 41 Ausländergesetz zu ändern, der bisher nur eine erkennungsdienstliche Behandlung vorsieht, wenn im Einzelfall Zweifel an der Identität des Ausländers bestehen. Es soll offenbar – über die Bürgerkriegsflüchtlinge hinaus – eine generelle Behandlung aller Ausländer angestrebt werden. Diese Maßnahme ist – ebenso wie die pauschale erkennungsdienstliche Behandlung von Asylbewerbern – unverhältnismäßig. Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat; daher muß sich auch jeder durch Dokumente ausweisen können. Erkennungsdienstliche Maßnahmen kommen aber nur in Betracht, wenn Zweifel an der Identität bestehen. Dieser Grundsatz muß auch gegenüber Asylbewerbern und Bürgerkriegsflüchtlingen gelten. Auch bei umfangreichsten Überwachungsmaßnahmen kann es keinen hundertprozentigen Schutz vor Rechtsmißbrauch geben. Es darf keine totale Erfassung geben, die Menschen miterfaßt, die sich gesetzeskonform verhalten. Erst bei Anhaltspunkten für Miß-

Der 2. Senat des Bundesverfassungsgerichts hat sich mit wesentlichen Teilen der Neufassung des Asylverfahrensgesetzes in mehreren Urteilen vom 14. Mai 1996 intensiv auseinandergesetzt. Alle wesentlichen Elemente wurden dort bestätigt. Daß nun gerade § 16 AsylVfG mit dem Menschenbild des Grundgesetzes und der Europäischen Menschenrechtskonvention nicht vereinbar sein sollte, bedürfte zumindest einer näheren Begründung.

Das Einbringen einer Vorlage zur Änderung des Ausländergesetzes durch den Berliner Senat ist entbehrlich. Die Regierung des Freistaates Bayern ist bereits in Absprache mit der Senatsverwaltung für Inneres Berlin und anderen Ländern initiativ geworden und hat zum Gesetzentwurf des Bundestages zur Änderung straf-, ausländer- und asylverfahrensrechtlicher Vorschriften (BT-Drs. 13/4948) einen entsprechenden Antrag eingebracht. Nach einem neu zu schaffenden § 41 a Ausländergesetz soll danach die Identität eines Ausländers aus einem Kriegs- oder Bürgerkriegsgebiet, der das 14. Lebensjahr vollendet hat, durch erkennungsdienstliche Maßnahmen gesichert werden, sofern ihm eine Aufenthaltsbefugnis oder eine Duldung erteilt werden soll oder seine Zurückschiebung oder Abschiebung in Betracht kommt. Diese Vorschrift orientiert sich im wesentlichen an § 16 Asylverfahrensgesetz.

Nach der Begründung des Antrages soll die erkennungsdienstliche Behandlung vor allem der Vermeidung von Mißbrauch, insbesondere von mehrfachem Leistungsbezug, dienen.

Der Gesetzentwurf ist vom Bundesrat beschlossen worden.

47 JB 1992, Anlage 2.3
48 JB 1991, 3.4.4
49 JB 1994, 4.6.3; Antwort auf die Kleine Anfrage Nr.5885, LPD vom 29. Dezember 1994
50 JB 1994 aaO
51 Stellungnahme des Senats zum Jahresbericht 1994, Drs. 12/5784
52 Drs. 13/576; Beschlußempfehlung Drs. 13/1027; Protokoll der Sitzung des Abgeordnetenhauses vom 14. November 1996, lfd. Nr.19 I

brauch von staatlichen Leistungen kommt die Anfertigung von erkennungsdienstlichen Unterlagen in Frage.

Ungeachtet dessen ist nicht erkennbar, wie die erkennungsdienstliche Behandlung zur Verhinderung des mißbräuchlichen Bezuges von Sozialleistungen beitragen soll. Hierfür wären eine erkennungsdienstliche Behandlung durch die Sozialleistungsträger und ein entsprechender Abgleich mit gespeichertem erkennungsdienstlichem Material durch diese Stellen erforderlich und im Sozialgesetzbuch vorzusehen. Abgesehen von der fehlenden technischen Infrastruktur wären die Mitarbeiter der Sozialämter mit dem daktyloskopischen Vergleich sicher überfordert.

Die Behauptung, es „soll offenbar – über die Bürgerkriegsflüchtlinge hinaus – eine generelle Behandlung aller Ausländer angestrebt werden“, entbehrt jeder Tatsachengrundlage.

Die Behandlung aller Ausländer aus einem Kriegs- oder Bürgerkriegsgebiet, die das 14. Lebensjahr vollendet haben, durch erkennungsdienstliche Maßnahmen, sofern ihnen eine Aufenthaltsbefugnis oder eine Duldung erteilt werden soll oder seine Zurückschiebung oder Abschiebung in Betracht kommt, ist entgegen den Ausführungen des Datenschutzbeauftragten zur Vermeidung von Mißbrauch geeignet und verhältnismäßig.

Es liegt in der Natur der Sache, daß Flüchtlinge häufig über keine Ausweisdokumente verfügen. Nur wenn die gesamte Gruppe von Flüchtlingen erkennungsdienstlich behandelt wird, sind Mehrfachantragsteller, die bei verschiedenen Ausländerbehörden vortragen, ohne Dokumente geflohen zu sein, und mit den dort ausgestellten fälschungssicheren Dokumenten bei verschiedenen Sozialleistungsträgern Leistungen beantragen, durch die Ausländerbehörden zu erkennen. Der mißbräuchliche Bezug von Sozialleistungen wird schon dadurch verhindert, daß ohne die vorherige Vorsprache eines Flüchtlings bei der Ausländerbehörde keine Sozialleistungen gewährt werden.

Vorbeugende Straftatenbekämpfung

Die erkennungsdienstliche Behandlung ist nicht nur Mittel zur Identitätsfeststellung und Aufklärung von Straftaten, sondern auch Hilfsmittel für die *Bekämpfung künftiger Straftaten*. Die Polizei kann zur vorbeugenden Bekämpfung von Straftaten erkennungsdienstliche Maßnahmen vornehmen, wenn der Betroffene verdächtig ist, eine Straftat begangen zu haben, und wegen der Art oder Begehensweise der Tat die Gefahr der Begehung weiterer Straftaten besteht (§ 23 Abs. 1 Nr. 2 ASOG). In ihrer Zweckbestimmung deckt sich diese Befugnis mit der strafprozessualen Vorschrift des § 81 b 2. Alternative StPO, der die Anfertigung von Lichtbildern und Fingerabdrücken „für Zwecke des Erkennungsdienstes” zuläßt. Bei beiden Normen ist das öffentliche Interesse an der Aufbewahrung der erkennungsdienstlichen Unterlagen abzuwägen gegen die Beeinträchtigung des Betroffenen. Wenn der Tatverdacht gegen ihn ausgeräumt ist, kommt eine weitere Aufbewahrung der Unterlagen nicht in Betracht. Die Prognose, ob die Gefahr der Begehung weiterer Straftaten besteht, hat sich auf konkrete Anhaltspunkte zu stützen. Eine schematische Verfahrensweise bei der Entscheidung über die Aufbewahrung erkennungsdienstlicher Unterlagen scheidet damit aus.

Die Fingerabdrücke und Fotografien werden nicht nur bei dem Berliner *Landeskriminalamt*[53], sondern auch bei dem *Bundeskriminalamt* vorgehalten. Die gespeicherten Daten unterliegen bundesweit dem Zugriff aller Polizeidienststellen, die an die Erkennungsdienst-Datei und die Datei Daktyloskopie angeschlossen sind.

Gerade erkennungsdienstliche Unterlagen zur vorbeugenden Straftatenbekämpfung waren in der Vergangenheit immer wieder Anlaß für Beanstandungen. So werden *Razzien* oft als willkommene Gelegenheit genutzt, an Fotos Betroffener zu gelangen:

Bei unseren ersten Prüfungen der Datei „Zuhälterei, Menschenhandel u.ä. Delikte”, damals noch „Prostituiertenkartei” genannt, fanden wir auch *Fotos von Prostituierten*, die die Frauen zum Teil auf diskriminierende Weise mit Ganzkör-

[53] vgl. JB 1991, 3.4.1

Bericht des Berliner Datenschutzbeauftragten	Stellungnahme des Senats

peraufnahmen zeigten[54]. Ungeachtet der Frage, unter welchen Voraussetzungen die Registrierung der Prostituierten, die sich keiner Straftat verdächtig gemacht haben, in der Datei zulässig ist, ist jedenfalls die Aufnahme und Aufbewahrung der Fotos zur vorbeugenden Straftatenbekämpfung unzulässig. Die Aufnahme der Fotos konnte nicht auf § 81 b 2. Alternative StPO gestützt werden, da hiervon nur Beschuldigte einer Straftat betroffen sein können. Die Frauen haben sich jedoch keiner Straftat verdächtig gemacht. Prostitution ist nicht strafbar. Auf § 23 Abs. 1 Nr. 1 ASOG konnten diese Maßnahmen ebenfalls nicht gestützt werden, da die Identität der Betroffenen feststellbar war. Auch wenn eine Fotoaufnahme zur Identitätsfeststellung erforderlich gewesen sein sollte, ist jedenfalls eine zweckentfremdende Speicherung zur vorbeugenden Straftatenbekämpfung gemäß § 42 Abs. 2 Satz 2 ASOG unzulässig, da die Datenerhebung, d.h. die Fotoaufnahme, zu diesem Zweck gemäß § 23 Abs. 1 Nr. 2 ASOG nur bei Verdächtigen einer Straftat zulässig ist. In der Datei sind seit unseren ersten Prüfungen keine Fotos von Prostituierten mehr enthalten.

Auf keinen Fall kann die Polizei beliebig bei Überprüfungen erkennungsdienstliche Maßnahmen bei allen Personen, die einmal einer Straftat verdächtig waren, vornehmen. Der Anwendungsbereich des § 23 Abs. 1 Nr. 2 ASOG ist beschränkt auf Personen, die – z.B. wegen Schuldunfähigkeit oder bereits erfolgter Verurteilung – nicht Beschuldigte sein können, bei denen aber im übrigen die tatbestandsmäßigen Voraussetzungen des § 81 b 2. Alternative StPO vorliegen. Die Maßnahme muß insbesondere inhaltlich und zeitlich im Zusammenhang mit einem Tatverdacht stehen. Die erkennungsdienstliche Behandlung nur aufgrund eines möglicherweise Jahre zurückliegenden Tatverdachts wie im ersten Fall ist nicht gerechtfertigt. Anderenfalls könnte der Verdacht entstehen, daß Ziel der Maßnahme nicht die Aufbewahrung der Unterlagen zum Zweck der vorbeugenden Straftatenbekämpfung ist, sondern die Durchführung der erkennungsdienstlichen Behandlung vor allem als Abschreckung dienen soll.

Es ist *unverhältnismäßig*, Delikte von unbedeutendem Gewicht, wie z.B. Ladendiebstahl, als Anlaßtat für eine erkennungsdienstliche Behandlung zur vorbeugenden Straftatenbekämpfung und eine jahrelange, bundesweite Speicherung der Daten zu nehmen. In diesen Fällen hat das Schutzbedürfnis der Allgemeinheit gegenüber dem Persönlichkeitsrecht der Betroffenen zurückzutreten. Im übrigen dürfte es gerade bei den meisten Bagatelldelikten an der Geeignetheit der erkennungsdienstlichen Behandlung fehlen, da dies die Prognose voraussetzt, daß der Betroffene Straftaten unter Täuschung oder Verschleierung seiner Identität begehen wird.

Es trifft zu, daß die Polizei nicht beliebig Personen erkennungsdienstlich behandeln darf, die einmal wegen einer Straftat verdächtig waren. Das sieht § 23 Abs. 1 ASOG nicht vor und das entspricht auch nicht der Vorgehensweise der Polizei.

Die Behauptung des Berliner Datenschutzbeauftragten, es könne der Verdacht entstehen, Ziel der erkennungsdienstlichen Behandlung sei vor allem die Abschreckung, ist aber in keiner Weise durch seine Aufgaben gedeckt und mit seiner Pflicht zur unparteiischen Amtsführung nicht zu vereinbaren. Im Kern enthält diese Aussage die Unterstellung, die Polizei würde bewußt rechtswidrig erkennungsdienstliche Maßnahmen durchführen, um die Betroffenen einzuschüchtern.

Der Auffassung des Berliner Datenschutzbeauftragten, es sei unverhältnismäßig, Delikte von unbedeutendem Gewicht als Anlaßtat für eine erkennungsdienstliche Behandlung zu nehmen, ist nicht zu folgen.

Nach der Rechtsprechung des Bundesverwaltungsgerichts setzen erkennungsdienstliche Maßnahmen nach § 81 b Alternative 2 StPO, der wie § 23 Abs. 1 Nr. 2 ASOG Maßnahmen zur vorbeugenden Bekämpfung von Straftaten regelt, nicht voraus, daß die Anlaßtat ein besonderes hohes Maß der Gemeinschädlichkeit aufweist. Der Senat ist darüber hinaus der Auffassung, daß allein aus dem Umstand, daß der Gesetzgeber bestimmte Verhaltensweisen unter Strafe gestellt hat, auf ein erhebliches öffentliches Interesse an der Verfolgung und Verhütung dieser Verhaltensweisen zu schließen ist. Außerdem läßt sich aus der kriminologischen Bezeichnung kein Rückschluß auf die Schwere und Bedeutung einer konkreten Tat ziehen. Auch Ladendiebstähle können gravierende Bedeutung haben, wenn sie serienmäßig begangen werden oder das erlangte Gut im Einzelfall von hohem Wert ist.

Unzutreffend ist ferner die Behauptung des Berliner Datenschutzbeauftragten, daß eine erkennungsdienstliche Maßnahme nur geeignet ist, wenn die Erwartung besteht, der Betroffene werde Straftaten unter Täuschung oder Verschleierung seiner Identität begehen. Es reicht aus, daß erkennungsdienstliche Unterlagen Ermittlungen fördern können. Das ist bei Lichtbildern schon der Fall, wenn eine Lichtbildvorlage zur Identi-

[54] JB 1992, 4.2.2

Unverhältnismäßig kann auch die *Art der Fotos* sein und damit zur Unzulässigkeit der erkennungsdienstlichen Maßnahme führen. Wenn in dem eingangs geschilderten Fall rumänische Abschiebehäftlinge mit Jacken ohne Reißverschluß, mit entblößter Brust und zerrissenen Kleidungsstücken auf erkennungsdienstlichen Fotos abgebildet werden, ist dies menschenverachtend, unverhältnismäßig und die Aufbewahrung der Fotos unzulässig. Die Lichtbilder wurden – offensichtlich in erheblicher Anzahl – gleichwohl in die Sammlung eingestellt. Erstaunlich an dem Vorgang ist, daß eine Vielzahl von Personen dabei beteiligt gewesen sein mußte, die die offensichtliche Rechtswidrigkeit der Maßnahme nicht erkannte. Ihnen konnte der Zustand der Betroffenen bzw. der ihrer Bekleidung nicht verborgen geblieben sein. Hinzu kommt, daß nicht erkannt wurde, daß Ganzkörperaufnahmen von Personen, die – zumal beschädigte – Bekleidungsstücke aus Polizeibeständen tragen, für Zwecke des Erkennungsdienstes völlig unbrauchbar sind. Die Lichtbilder hätten spätestens mit der Erkenntnis, daß sie rechtswidrig erhoben und rechtswidrigerweise in die Lichtbildsammlung eingestellt wurden, vernichtet werden müssen (§ 48 Abs. 2 Nr. 1 ASOG). Dies ist nicht geschehen. Wir haben daher die unverzügliche Durchsicht der gesamten Lichtbildkartei mit dem Ziel empfohlen, die rechtswidrig erhobenen und gespeicherten Daten zu löschen bzw. zu vernichten. Dazu sieht sich die Polizei aber aus personellen Gründen nicht in der Lage. Es wurde jedoch zugesagt, daß mit der Einführung des automatisierten Verfahrens für die Lichtbildkartei eine Gesamtdurchsicht und Vernichtung nicht zulässig angefertigter Bilder erfolgt.

3.2 Erforschung der DDR-Vergangenheit

Auch im Jahre sieben der deutschen Einheit sind in den Medien, von Politikern, aber auch in persönlichen Gesprächen der Bürger deutlich Meinungen zu vernehmen, daß die Geschichte der Entstehung und Vertiefung der deutschen Teilung, insbesondere aber die Geschichte der DDR noch nicht hinreichend aufgearbeitet wurde. Die Bedeutung einer solchen, den Grundsätzen der Objektivität, der wissenschaftlichen Unabhängigkeit und – so schwer es gerade bei zeitgeschichtlicher Forschung erscheinen mag – der Neutralität folgenden Aufarbeitung durch die Forschung kann im Hinblick auf die Gestaltung der inneren Einheit Deutschlands kaum hoch genug eingeschätzt werden.

Zeitgeschichtliche Forschung ist ohne den Zugang zu Akten unmöglich. Diese Akten enthalten aber vielfache Informationen über noch lebende Personen. Im Herbst 1989 gelang es, die in jahrzehntelanger Schnüffelwut angehäuften Daten des ehemaligen Ministeriums für Staatssicherheit und vieler anderer Dienststellen der ehemaligen DDR in wesentlichen Teilen vor der Vernichtung zu bewahren und damit nicht nur für die Betroffenen, sondern auch für die zeitgeschichtliche Forschung zur Aufarbeitung dieses Teils der deutschen Geschichte zu retten. Der Bundesgesetzgeber hat eine sehr großzügige Regelung für die Verwendung der Stasi-Unterlagen für die Aufarbeitung der Tätigkeit des Ministeriums für Staatssicherheit durch die wissenschaftliche Forschung in das *Stasi-Unterlagengesetz* (§§ 32, 33

fizierung unbekannter Täter führen kann, egal ob sie ihre Identität verschleiern oder den möglichen Zeugen ganz einfach nicht von Namen bekannt sind. Darüber hinaus gehören zu den erkennungsdienstlichen Unterlagen auch Fingerabdrücke. Diese sind zur Förderung von Ermittlungen immer geeignet, wenn nicht auszuschließen ist, daß der Betroffene bei der Begehung weiterer Taten Fingerabdruckspuren hinterläßt. Auch insoweit ist es völlig unerheblich, ob er über seine Identität täuscht oder diese verschleiert.

Siehe obige Ausführungen zu Ziffer 3.1 – Erkennungsdienstliche Behandlung.

und 42) aufgenommen. Personenbezogene Daten werden dabei nicht pauschal geschützt, sondern es wird nach Tätern und Opfern unterschieden. Damit wurde ein Weg gefunden, der einen Ausgleich zwischen den widerstreitenden Grundrechten auf informationelle Selbstbestimmung, der Forschungsfreiheit sowie der Pressefreiheit und der Freiheit der Berichterstattung bewirken kann.

Auch im *Bundesarchivgesetz* wurde für die Nutzung der Archivalien der Parteien und Massenorganisationen der DDR, soweit sie die Wahrnehmung staatlicher Aufgaben betrafen, eine Sonderregelung erlassen, welche die sonst für Bundesarchivgut geltende Schutzfrist von 30 Jahren aufhebt. Für die Nutzung von personenbezogenem Archivgut gelten jedoch einheitliche Schutzfristen, aber auch eine einheitliche Privilegierung des wissenschaftlichen Zugangs zu Daten über Personen, die als *Personen der Zeitgeschichte und Amtsträger* gelten, ist vorgesehen. Für deren personenbezogenen Daten, die in Ausübung ihres Amtes entstanden sind, können für die Forschung die Schutzfristen verkürzt werden. Schutzlos sind diese Personen aber nicht. Es sind auch deren schutzwürdigen Belange als Betroffene angemessen zu berücksichtigen.

Der Berliner Gesetzgeber hat mit dem *Berliner Archivgesetz* (ArchGB) eine Regelung geschaffen, die Unterlagen von ehemaligen Einrichtungen der DDR sichert, welche ihrer Bestimmung nach für Verwaltungszwecke entstanden sind, die heute von öffentlichen Stellen des Landes wahrzunehmen sind. Sind diese Unterlagen für die Verwaltung heute nicht mehr erforderlich bzw. steht nicht zu befürchten, daß schutzwürdige Belange eine weitere Aufbewahrung dort notwendig machen, sind diese Unterlagen dem Landesarchiv anzubieten. Wenn das Landesarchiv die Übernahme ablehnt, sind die Unterlagen zu vernichten. Auch das Landesarchivgesetz legt für die Nutzung der Archivalien Schutzfristen fest, schafft aber zugleich die Möglichkeit eines privilegierten Zuganges für die Forschung.

Manche öffentliche Stellen in Berlin unterhalten eigene Archive. Die Universitäten und Hochschulen beispielsweise bestimmen per Satzung unter sinngemäßer Anwendung des Landesarchivgesetzes die Grundsätze ihrer eigenen Archive. Auch hier wird der privilegierte Zugang durch die wissenschaftliche Forschung gesichert.

Im Frühsommer des Jahres 1995 wurde durch eine recht kontroverse Diskussion in der Presse die Öffentlichkeit auf vermutete Beschränkungen der Forschungsfreiheit bei der Nutzung des Archivs der Humboldt-Universität aufmerksam gemacht.

Im Jahre 1992 hatte sich ein Forscher, der nicht Mitglied der Humboldt-Universität war, um ein Forschungsprojekt bemüht, bei dem ein ganzer Fachbereich sowie einzelne gegenwärtige und frühere Mitglieder des Fachbereiches Untersuchungsgegenstand sein sollten. Es war vorgesehen, die diesbezüglichen personenbezogenen Unterlagen der „Gauck-Behörde" entsprechend den privilegierten Regelungen für Forscher zu nutzen. Nachdem dieses Projekt nicht zustande gekommen war, bemühte sich der Forscher, das angestrebte Thema im Rahmen einer Dissertation zu bearbeiten, bei der er nunmehr das Archiv der Humboldt-Universität nutzen wollte.

Im Januar 1994 nahm der Forscher mit dem Archiv Kontakt auf. Dort wurde er auf die 30-jährige Sperrfrist nach dem Landesarchivgesetz verwiesen, die jedoch durch eine Ausnahmeregelung des Dekans der betreffenden Fakultät aufgehoben werden könne. Diese Genehmigung wurde nicht erteilt. Somit wandte sich der Wissenschaftler an die Präsidentin der Humboldt-Universität. Die Präsidentin bat, Widersprüche und Mißverständnisse in Rücksprache mit der Fakultät auszuräumen und das Projekt deutlicher zu begründen. Hierzu erklärte der

Forscher, daß sein Dissertationsvorhaben sich nach seiner Zweckbestimmung nicht auf natürliche Personen beziehe. Eine Begründung, warum der Zugang zu Daten natürlicher Personen unerläßlich sei, erfolgte jedoch nicht. Der behördliche Datenschutzbeauftragte der Humboldt-Universität legte daraufhin dem Wissenschaftler dar, daß ein Datenzugang nur nach Nachweis eines besonderen öffentlichen Interesses zu genehmigen sei. Dieses leitete der Wissenschaftler nunmehr allein aus dem Interesse an der wissenschaftlichen Aufarbeitung der politischen Vorgänge während der Zeit der SED-Herrschaft her. Auch in einem erneuten Antrag wurde nach allgemeiner Darlegung des Forschungsprojektes auf ein generelles erhebliches öffentliches Interesse an der Aufarbeitung der SED-Diktatur verwiesen. Ziel und Zweck der Recherche im Archiv sei die Sichtung und Einordnung archivalischer Hinterlassenschaften der ehemaligen Sektion. Die Humboldt-Universität beauftragte einen renommierten Wissenschaftler zu begutachten, ob mit diesem Antrag belegt werden würde, warum dieses Thema im besonderen öffentlichen Interesse liege, und ob dies eine Ausnahmeregelung begründen würde. Bei Würdigung der sich auftuenden präziseren Konturen des Forschungsprojektes erschien dem Gutachter das besondere öffentliche Interesse zumindest fragwürdig. Es blieb bei der Ablehnung.

Grundsätzlich dürfen Unterlagen nach § 8 Abs. 2 ArchGB nicht vor Ablauf von 30 Jahren nach deren Entstehung durch Dritte genutzt werden. Dies gilt auch für Unterlagen, die in der ehemaligen DDR entstanden sind und sich heute rechtmäßig in der Obhut öffentlicher Stellen des Landes Berlin befinden. Es erfolgt eine Gleichbehandlung. Ausnahmen von der allgemeinen Schutzfrist bedürfen der pflichtgemäßen Abwägung der berechtigten Interessen. So ist festgelegt, daß Archivgut, welches sich nach seinem wesentlichen Inhalt auf natürliche Personen bezieht, nur mit deren Einwilligung zugänglich gemacht werden darf. Für die Verkürzung von Schutzfristen setzt der Gesetzgeber ein „überwiegendes öffentliches Interesse" voraus. Ein überwiegendes öffentliches Interesse an der Nutzung von Archivgut vor Ablauf der Schutzfrist liegt nur dann vor, wenn die Person oder der historische Vorgang, auf die in dem gesperrten Archivgut Bezug genommen wird, von besonderer oder exemplarischer Bedeutung für die Erforschung der Geschichte oder das Verständnis der Gegenwart ist (§ 8 Abs. 5 ArchGB).

Der Wissenschaftler hat darzulegen, daß das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen *erheblich* überwiegt.

Ein kurzer verbaler Verweis auf den exemplarischen Charakter sowie die Skizzierung des wissenschaftlichen Projektes durch den Forscher können nicht genügen, um die Persönlichkeitsrechte der Betroffenen, „hinter deren Rücken" geforscht werden soll, einzuschränken. Die Darlegungslast hinsichtlich der wissenschaftlichen und das Allgemeininteresse betreffenden Wertung von Forschungsvorhaben liegt beim Forscher. Die Stelle, die in das Recht auf informationelle Selbstbestimmung eingreifen möchte, hier also die Hochschule, die ohne Einwilligung der Betroffenen deren personenbezogenen Daten für die Forschung öffnen soll, steht in der Verpflichtung, diesen Eingriff zu rechtfertigen. Sie kann sich nicht damit begnügen, auf die Behauptung eines Forschungsinteresses durch den Forscher zu verweisen.

Ein wissenschaftliches Interesse an der Durchführung eines Forschungsvorhabens hat als solches gegenüber der informationellen Selbstbestimmung eines jeden Betroffenen noch keinen Vorrang. Das öffentliche Forschungsinteresse muß vielmehr erheblich überwiegen. Auch bei Prüfungsarbeiten bzw. anderen

Qualifikationsnachweisen, wie diese auch Dissertationen darstellen, ist dies nicht vornherein der Fall. Nach § 35 Berliner Hochschulgesetz (BerlHG) dient eine Promotion dem Nachweis der Befähigung zu vertiefter wissenschaftlicher Arbeit. Allein die Einordnung des § 35 BerlHG in den 3. Abschnitt des Berliner Hochschulgesetzes – Studium, Lehre und Prüfungen – und nicht in den 4. Abschnitt – Forschung – zeigt, daß eine Inanspruchnahme des Forschungsprivilegs beim Zugang zu personenbezogenen Daten zum Zwecke der Erstellung von Dissertationen nur in Ausnahmefällen gegeben sein kann.

Die Ablehnung des Zugangs zum Archiv der Humboldt-Universität war daher datenschutzrechtlich korrekt. Dies haben wir auch der Senatsverwaltung für Wissenschaft und Kulturelle Angelegenheiten mitgeteilt, die die Präsidentin der Hochschule aufgefordert hatte, ihre Entscheidung zu revidieren.

Neben der unmittelbaren Erforschung der DDR-Vergangenheit anhand von Originalunterlagen widmet sich die zeitgeschichtliche Forschung auch zunehmend der *Analyse der Bewältigung dieser Vergangenheit im vereinten Deutschland.* Im Rahmen eines Drittmittelforschungsprojektes der juristischen Fakultät der Humboldt-Universität besteht eine Aufgabe darin zu untersuchen, wie die heutige Justiz auf ein Verhalten reagiert, das in einem anderen Systemzusammenhang stand und welches von Inhabern der Staatsmacht ausging oder jedenfalls von diesen gebilligt wurde. So ist vorgesehen, alle im Zusammenhang mit der sogenannten Regierungskriminalität der DDR ergangenen Urteile, aber auch Anklageschriften und Einstellungsverfügungen zu sammeln und für die Forschung zu erschließen. Zunächst wurde klar, daß durch die Justizverwaltungen Berlins und der neuen Bundesländer diese Unterlagen nicht hinreichend anonymisiert bereitgestellt werden können. Wollte man die Verarbeitung von der Einwilligung der Betroffenen abhängig machen, wäre ein solches Projekt von Anfang an zum Scheitern verurteilt. Bereits im Antrag zum Forschungsprojekt wurde ausführlich und hinreichend bestimmt dargelegt, daß das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck dieser Forschung auf eine andere Weise nicht erreichbar ist.

Nach ausführlicher datenschutzrechtlicher Beratung durch unsere Behörde wurden Wege gefunden, die die Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen deutlich mildern, aber den Zweck der Forschung nicht gefährden. Nach Zustimmung der Senatsverwaltung für Justiz sowie der Justizministerien der anderen neuen Bundesländer senden die Justizverwaltungen die entsprechenden Unterlagen an die Berliner Staatsanwaltschaft. Durch besonders ausgewählte Hilfskräfte werden in Räumen der Staatsanwaltschaft diese Unterlagen anonymisiert. Das geschieht durch Kopieren der Originalunterlagen und deren sofortige Rückgabe. Die Kopien werden nachfolgend durch Schwärzen anonymisiert und dann erneut kopiert. Nur die Zweitkopien werden dann den Forschern der Humboldt-Universität zur Verfügung gestellt. Die Hilfskräfte sind datenschutzrechtlich besonders verpflichtet und bezüglich ihrer sonstigen Tätigkeit nicht mit dem Projekt verbunden. Dieses Verfahren wurde sowohl von den Justizministerien als auch den Datenschutzbeauftragten der neuen Bundesländer gebilligt. Auch künftig werden wir dieses Forschungsvorhaben datenschutzrechtlich weiter begleiten und kontrollieren.

Gemeinsam mit den Berliner Stellen, die über Daten aus DDR-Zeiten verfügen, und auskunftsbegehrenden Wissenschaftlern bemühten wir uns, für eine Reihe *weiterer Forschungsvorhaben* datenschutzrechtlich akzeptable Lösungen zu finden. Beispielhaft seien hier nur erwähnt eine Studie über Tötungsde-

Der Senat sieht die Zusammenarbeit und das gefundene datenschutzrechtliche Verfahren beim Forschungsprojekt „Strafjustiz und DDR-Vergangenheit“ der Humboldt-Universität als vorbildlich an. Hier konnte im Interesse der wissenschaftlichen Aufbereitung von Gegenwart und Vergangenheit ein praktikabler Weg gefunden werden.

likte in den Jahren 1985 bis 1990, die Einsichtnahme in Unterlagen zum Havemann-Prozeß, um zu klären, in welchem Umfang in der Justizpraxis der DDR die Urteile der Gerichte von den Anträgen der Staatsanwaltschaft abwichen, eine Untersuchung über die soziale Herkunft der Studentenschaft der Humboldt-Universität bis 1967, eine Analyse von Familienrechtssachen an DDR-Gerichten, eine Vergleichsstudie zum Schulsystem in Ost- und Westdeutschland sowie eine Untersuchung auf Grundlage einer DDR-Studie über „sehr kleine Frühgeborene".

Amts- und Funktionsträger der DDR und Personen der Zeitgeschichte

Ende des Jahres 1995 bat uns der Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR in Berlin um datenschutzrechtliche Beratung und Unterstützung für eine *Studie zur Entwicklung des Grenzregimes* von 1949 bis zum ersten Passierscheinabkommen 1964. Dazu wurde durch die Forscher ein Antrag auf Einsichtnahme in die Unterlagen des ehemaligen Bezirksverwaltungsarchivs des Präsidiums der Volkspolizei Berlin gestellt. Der Polizeipräsident lehnte dies mit dem Verweis darauf ab, daß der Zweck der Forschung auch ohne Einsicht in personenbezogene Daten erreicht werden könne und damit das für den privilegierten Zugang geforderte erheblich überwiegende öffentliche Interesse nicht vorliegen würde. Zunächst prüften wir im Archiv des ehemaligen Präsidiums der Volkspolizei Berlin die Sachlage. Nach stichprobenhafter Einsicht in die Unterlagen stellten wir fest, daß eine Trennung von personenbezogenen sowie von Sachinformationen technisch nicht durchführbar ist. Durch die gezielte Auswahl der Archivalien hätten die Eingriffe bei der Akteneinsicht entschieden gemildert werden können. Die Namen der DDR-Amtsträger waren jedoch bei diesem Projekt für die Analyse der funktionsbezogenen Befehlsstrukturen innerhalb der Volkspolizei und der Einflußnahmen des Ministeriums für Staatssicherheit unabdingbar. Eine Nutzung weiterer möglicherweise vorhandener personenbezogener Daten zu anderen Zwecken als der Analyse von Befehlsstrukturen war nicht vorgesehen.

In der Forschungsklausel des Berliner Datenschutzgesetzes für die Offenbarung personenbezogener Daten ohne Einwilligung der Betroffenen werden zwei Bedingungen nebeneinandergestellt. Zum einen ist dies das vom Forscher nachzuweisende erheblich überwiegende öffentliche Interesse und zum anderen die ebenfalls nachzuweisende Unmöglichkeit, den Zweck der Forschung auf andere Weise zu erreichen. Da es bei diesem Forschungsprojekt lediglich um die Nutzung der Namen von Amtsträgern für eine Strukturanalyse ging, waren die Anforderungen geringer anzusetzen. Die Innenverwaltung beharrte gleichwohl auf ihrer Ablehnung und teilte uns mit, daß, um Befehlsstrukturen innerhalb der Volkspolizei zu erkennen, nicht in erster Linie die Namen der Funktionsträger von Interesse sind, sondern deren Stellung im System. Auch wurde dargelegt, daß das Berliner Datenschutzgesetz nicht danach differenziert, ob es sich bei den personenbezogenen Daten um solche von Amtsträgern oder um Daten Geschädigter handelt.

Das von der Innenverwaltung dargelegte datenschutzrechtliche Problem ist also, ob Personen, die als *Amts- oder Funktionsträger* tätig sind oder waren, den Schutz des informationellen Selbstbestimmungsrechts in vollem Umfang für sich in Anspruch nehmen können. Unbestritten dürfte sein, daß dieses Grundrecht auch für den einzelnen Amts- oder Funktionsträger in seinem Verhältnis zum Staat als „Gewaltunterworfener" gilt. Zu beachten ist, daß die Trennlinie zwischen dienstlicher Tätigkeit und dem Abhängigkeitsverhältnis der Beschäftigten gegenüber dem Arbeitgeber/Dienstherrn, das eindeutig dem Datenschutz unterliegt, nicht immer eindeutig gezogen werden

In seinem Antrag vom August 1995 hat der Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR ausdrücklich darauf hingewiesen, daß für das geplante Forschungsvorhaben kein Bedarf an speziell personenbezogenen Daten vorhanden ist. Nach § 30 Abs. 1 Nr. 2 des Berliner Datenschutzgesetzes dürfen zum Zwecke wissenschaftlicher Forschung personenbezogene Daten ohne Einwilligung des Betroffenen nur für bestimmte Forschungsvorhaben übermittelt werden, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

Ein überwiegendes öffentliches Interesse an der Übermittlung personenbezogener Daten war aber schon nach dem Antrag des Landesbeauftragten nicht gegeben. Das Berliner Datenschutzgesetz differenziert nicht danach, ob es sich bei den personenbezogenen Daten um solche von Amtsträgern oder um Daten von Geschädigten handelt. In beiden Fällen sind an das überwiegende öffentliche Interesse die gleichen Anforderungen zu stellen. Ferner wäre der Zweck der Forschung hier auch auf andere Weise erreichbar gewesen, nämlich durch Einsichtgewährung in Akten, die durch Umkopieren, Schwärzen oder ähnliche Maßnahmen von personenbezogenen Daten bereinigt wurden.

Deshalb hat sich die zuständige Senatsverwaltung nicht in der Lage gesehen, der Übermittlung personenbezogener Daten für diese Forschungsarbeit zuzustimmen. Dabei ist auch zu berücksichtigen, daß die unbefugte Übermittlung personenbezogener Daten mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird.

kann. Im Zusammenhang mit DDR-Unterlagen soll hier insbesondere auf bestimmte „gesellschaftliche" Aktivitäten der Beschäftigten und Funktionsträger verwiesen werden. Die Grundrechte einschließlich des Rechts auf informationelle Selbstbestimmung entfalten ihren Schutz vor allem, wenn die betreffenden Personen von staatlicher Gewaltausübung betroffen sind. Soweit sie als Amts- oder Funktionsträger in Ausübung hoheitlicher Gewalt gegenüber Dritten handeln, müssen sie Beschränkungen hinnehmen. Die staatliche Tätigkeit als solche steht nicht unter dem Schutz der Grundrechte. Die wissenschaftliche Nutzung oder die anderweitige Einsicht in staatliche Verwaltungsunterlagen bedarf somit keiner besonderen gesetzlichen Grundlage. Im Unterschied dazu ist diese für die Einsicht in Personalakten oder für eine personenbezogene Analyse der individuellen Amtsausübung erforderlich.

Datenschutzrechtlich problematisch ist bei der Erforschung der DDR-Vergangenheit, daß der Tätigkeit der damaligen Amts- und Funktionsträger, ob als Lehrer, Verwaltungsangestellter oder Polizist, nicht die heutige rechtsstaatliche Verfaßtheit der Bundesrepublik Deutschland zugrunde gelegt werden kann. Gründe, die eine Weiterbeschäftigung von Arbeitnehmern im öffentlichen Dienst der ehemaligen DDR einschließlich der Amts- und Funktionsträger nach dem Einigungsvertrag ausschlossen und daher ein Festhalten am Arbeitsverhältnis unzumutbar erscheinen ließen, wurden im Einigungsvertrag abschließend aufgeführt (Verstöße gegen die Grundsätze der Menschlichkeit und Rechtsstaatlichkeit oder frühere Tätigkeit für das Ministerium für Staatssicherheit). Die vielfältigen Überprüfungen im öffentlichen Dienst von ehemals Ostberliner Beschäftigten dürften gegenwärtig im wesentlichen abgeschlossen sein. Diese bei den Überprüfungen entstandenen oder genutzten Unterlagen einschließlich bestimmter, das heutige Arbeitsverhältnis nicht berührender Schriftstücke der alten „Kaderakten" müssen durch eine geschützte Ablage in einem verschlossenen Umschlag der regelmäßigen Personalsachbearbeitung entzogen werden. Eine wissenschaftliche Erforschung früherer und weitergeführter Arbeitsverhältnisse von öffentlichen Beschäftigten einschließlich ihrer früheren „gesellschaftlichen" Aktivitäten dürfte damit wegen der besonderen schutzwürdigen Belange der Betroffenen nur in seltenen Ausnahmefällen zu genehmigen sein. Sollen hingegen, wie im oben erwähnten, vom Berliner Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR begonnenen Projekt Strukturen auch mit Hilfe von Namen der Amts- und Funktionsträger untersucht werden, so steht dem, die Wissenschaftlichkeit der Untersuchung sowie ein überwiegendes öffentliches Interesse und die Unumgänglichkeit vorausgesetzt, aus datenschutzrechtlicher Sicht nichts entgegen.

Amts- und Funktionsträger, auch die der ehemaligen DDR, sind keinesfalls von vornherein bezüglich der Nutzung und Veröffentlichung ihrer Daten im Rahmen der zeitgeschichtlichen Forschung mit *Personen der Zeitgeschichte* gleichzusetzen. Das informationelle Selbstbestimmungsrecht von Personen der Zeitgeschichte tritt in dem Maße zurück, wie der eigene Anteil dieser Personen am Ereignis wächst. Wer in der Öffentlichkeit auftritt, dem muß auch die Veröffentlichung der näheren Umstände dieses Wirkens zugemutet werden können. Repräsentanten eines Staates, bekannte Sportler oder Schauspieler, aber auch in Anbetracht der deutschen Vergangenheit Personen, die sich schwerer Menschenrechtsverletzungen oder Verbrechen schuldig gemacht haben, können sich also nicht durch den Verweis auf das Recht auf informationelle Selbstbestimmung der Forschung entziehen oder einer Veröffentlichung der Ergebnisse im unerläßlichen Rahmen widersetzen. Personen, die

sich schwerer Menschenrechtsverletzungen schuldig gemacht haben, können lediglich nach ihrer strafrechtlichen Verfolgung durch ihr Recht auf Resozialisierung für sich in Anspruch nehmen, dann in der „Anonymität des Vergessens" zu versinken. Ein Amts- und Funktionsträger muß es zwar hinnehmen, daß seine Mitwirkung an hoheitlichen Maßnahmen (Unterschrift unter einem Bescheid) zum Gegenstand der Forschung gemacht und veröffentlicht wird. Er muß es aber – im Gegensatz zu Personen der Zeitgeschichte – in aller Regel nicht hinnehmen, daß seine Personalakte von Wissenschaftlern ausgewertet wird.

3.3 Datenschutz für Mieter

Viele Wohnungsbaugesellschaften, Genossenschaften und sonstige Vermieter speichern mittels umfangreicher *Fragebögen eine Fülle personenbezogener Daten von Wohnungsbewerbern*. Zahlreiche Bürger haben sich im Jahr 1996 über diese Praxis der Vermieter beschwert. Um das Verhalten der Vermieter bei der Erhebung und Speicherung von personenbezogenen Daten von Wohnungsbewerbern genauer überprüfen zu können, haben wir die größten Berliner Vermieter angeschrieben und um die Übersendung eines Fragebogens gebeten. Etwa 50 Vermieter sandten uns ihre Fragebögen zu. Bei der Überprüfung der verwendeten Fragebögen mußten wir feststellen, daß nur wenige den gesetzlichen Vorgaben entsprachen. Zu diesen führte das Amtsgericht Wiesbaden[55] aus:

„Den Mieter treffen Aufklärungspflichten nur für solche Umstände, die für den Vermieter bei objektiver Bewertung und Berücksichtigung schutzwürdiger Belange des Mieters der Auskunft bedürfen. Das ist bezüglich solcher Umstände zu bejahen, die für das Mietvertragsverhältnis wesentlich sind und deren Offenbarung dem Mieter zuzumuten ist. Fragen nach dem persönlichen Status des Mieters sind unzulässig, soweit sie sich nicht auf besondere Qualifikationsmerkmale beziehen, die den Mietgebrauch betreffen."

In einer Sitzung mit der Fachkommission für Recht des Verbandes Berlin-Brandenburgischer Wohnungsunternehmer e. V. haben wir dargestellt, welche personenbezogenen Daten nach diesen Vorgaben erhoben werden dürfen:

Einzelne Vermieter haben in ihren Fragebögen nach der *Religionszugehörigkeit* des Wohnungsinteressenten gefragt. Auch katholische oder evangelische Einrichtungen haben nicht das Recht, die Religionszugehörigkeit des Wohnungsinteressenten zu speichern. Einrichtungen, die die Religionszugehörigkeit eines Wohnungsinteressenten abfragen, versuchen offensichtlich, Wohnungen nur an Personen abzugeben, die einer bestimmten Religionsgemeinschaft (nämlich der des Wohnungsträgers) angehören. Während es im Arbeitsrecht anerkannt ist, daß Tendenzbetriebe bei Einstellungen überprüfen dürfen, ob ein Bewerber die Tendenz des Unternehmens glaubhaft nach außen vertritt, kennt das Mietrecht einen derartigen Tendenzschutz nicht, da ein Mieter einer religiösen Einrichtung in der Öffentlichkeit nicht als Vertreter der

[55] Wohnungswirtschaft und Mietrecht (WM) 1992, S. 597

Die Lebens- und Wohnsituation während der letzten Jahrzehnte hatte zur Folge, daß die Wohnungsbaugesellschaften vielfach ihre Position zur Erweiterung ihres Serviceangebotes für die Mieter nutzen. Die wohnungswirtschaftlichen Rahmenbedingungen unterstützten sie in ihrem Informationsbegehren.

Der Senat teilt die Auffassung des Berliner Datenschutzbeauftragten bezüglich des Umfangs der Datenerhebungen durch die Wohnungsbaugesellschaften insoweit, als er Fragen, die den Wohnungswechsel des Wohnungsbewerbers betreffen (z.B. Gründe für den Wohnungswechsel, Höhe des früheren Mietzinses usw.) ohne entsprechende Begründung (z.B. Strukturverwerfungen in Großsiedlungen) für nicht berechtigt hält. Der Senat weist darauf hin, daß die Wohnungsbaugesellschaften die Datenerhebungen selbständig und weitgehend unabhängig durchführen.

Soweit die Wohnungsbaugesellschaften aufgrund einer Kooperationsvereinbarung zwischen ihnen und dem Land Berlin für bestimmte Personengruppen Kontingente vorzuhalten haben, hält der Senat Datenerhebungen bei Wohnungsbewerbern durch die Gesellschaften insoweit für gerechtfertigt, als sie der Feststellung der Zugehörigkeit zu den betroffenen Personengruppen dienen. In diesen Fällen ist die Vornahme entsprechend detaillierter Abfragen nach Auffassung des Senats erforderlich.

Einrichtung angesehen wird. Religiöse Einrichtungen müssen es also hinnehmen, daß in ihren Wohnungen Mieter wohnen, die nicht ihrer Religionsgemeinschaft angehören.

Auf fast allen Fragebögen wurden die Daten *Geburtsort, Geburtsname, Geburtsdatum* abgefragt. Die Erhebung dieser Daten wurde damit begründet, daß größere Wohnungsbaugesellschaften so viele Bewerbungen von Mietinteressenten erhalten, daß es ohne diese Daten für sie nicht möglich sei, insbesondere die Bewerber, die einen häufig vorkommenden Namen haben, zu unterscheiden. Bei größeren Wohnungsbaugesellschaften ist es hinzunehmen, daß zur Unterscheidung der Mietinteressenten das Geburtsdatum gespeichert wird. Die Speicherung dieses Merkmals ist allerdings auch ausreichend, um selbst bei „Allerweltsnamen" eine ausreichende Unterscheidungsmöglichkeit der Mietinteressenten zu gewährleisten. Die zusätzliche Speicherung der Merkmale Geburtsort und Geburtsname ist zur Unterscheidung der Mietinteressenten nicht nötig. Die Frage nach dem Geburtsort oder dem Geburtsnamen ist somit rechtswidrig.

Wohnungsinteressenten müssen häufig angeben, welche Staatsangehörigkeit sie besitzen. Die Frage nach der Staatsangehörigkeit ist jedoch in der Regel rechtswidrig. Die Erhebung dieses Datums wurde damit begründet, daß man Ausländern keinen Wohnraum in ausländerfeindlichen Gegenden geben und ethnische Konflikte in einem Haus vermeiden wolle. Die Abfrage der *Staatsangehörigkeit* kann aber nicht verhindern, daß Mieter in ausländerfeindlichen Gegenden gefährdet sind. Ein Skinhead wird sich im Zweifel nicht darum kümmern, ob der Mieter ein Türke oder ein eingebürgerter ehemaliger Türke ist. Auch ethnische Konflikte in einem Haus werden hierdurch nicht verhindert. So haben z.B. Russen und Tschetschenen in der Regel denselben Paß. Ähnliche Probleme dürften bei Bosniern (Serben, Kroaten, Moslems) bestehen.

Teilweise wurde von Wohnungsbaugesellschaften die Befürchtung geäußert, ein Wohnkomplex, in dem sich zu viele Ausländer aufhalten würden, würde „umkippen". Die Gefahr wird gesehen, wenn in einem Haus zu viele Personen einer bestimmten ausländischen Nationalität wohnen. Hierbei wird übersehen, daß für die Stimmung der Mieter in einem Mietkomplex eher die Wohnqualität von Bedeutung ist als die nationale Zusammensetzung der Mieter.

Einige Wohnungsbauunternehmen fragen auf den Bewerberfragebögen *Personalausweisnummer, Paßnummer* und *ausstellende Behörde* des jeweiligen Dokumentes ab. Teilweise wird von dem zukünftigen Mieter sogar gefordert, eine Kopie des Personalausweises oder des Passes zu übersenden. Diese Daten werden von den Wohnungsbaugesellschaften in der irrigen Annahme gespeichert, mit Hilfe dieser Daten Mieter aufzuspüren, die mit einem Mietrückstand die Wohnung verlassen haben und sich nun an einem neuen Wohnsitz aufhalten. Nach den melderechtlichen Vorschriften (§ 28 Meldegesetz) benötigt der Vermieter weder Personalausweis- noch Paßnummer, um Auskunft über die gegenwärtige Anschrift zu erlangen. Auch für die möglicherweise notwendige Einleitung gerichtlicher Maßnahmen (Einleitung eines Strafverfahrens durch die Erstattung einer Strafanzeige, Klageerhebung vor dem Zivilgericht) werden weder die Personalausweisnummer noch die Paßnummer benötigt.

In der Mehrzahl der Fragebögen wurden die Wohnungsbewerber nach ihren *Motiven für den Wohnungswechsel* befragt. So wurden etwa Daten über die bisherige Wohnung, die Höhe des monatlichen Mietzinses, die Anschrift und die Telefonnummer des bisherigen Vermieters sowie die Dauer des bisherigen Miet-

verhältnisses gespeichert. Keine dieser Daten wird für den Abschluß eines Mietvertrages benötigt.

Der in der bisherigen Wohnung gezahlte monatliche Mietzins mag zwar ein Indiz dafür sein, welche Miethöhe sich der Wohnungsbewerber leisten kann, trotzdem ist der Aussagewert dieses Datums relativ gering. So dürfte es häufig der Fall sein, daß der Wunsch eines Mieters, eine neue Wohnung zu beziehen, im Zusammenhang mit einer Veränderung (positiv oder negativ) seiner finanziellen Möglichkeiten steht.

Die Auskünfte über den Vermieter sollen offensichtlich dazu benutzt werden, sich bei dem ehemaligen Vermieter nach dem Verhalten des Mieters zu erkundigen. Eine derartige Datenerhebung hinter dem Rücken des Betroffenem widerspricht dem Grundsatz von Treu und Glauben (personenbezogene Daten sollten grundsätzlich beim Betroffenen erhoben werden) und ist nach § 28 Abs. 1 Satz 2 BDSG rechtswidrig.

Die Frage nach dem Zeitraum des bisherigen Mietverhältnisses wird von den Wohnungsbaugesellschaften gestellt, weil man sich hierdurch Rückschlüsse auf die von dem Mieter angestrebte Länge des Mietverhältnisses erhofft. Grundsätzlich hat ein Vermieter aber kein Recht, von dem Mieter beim Abschluß eines unbefristeten Mietvertrages eine bestimmte Mindestvertragsdauer zu fordern. Aus diesem Grunde ist auch die Frage nach der bisherigen Vertragsdauer seiner Mietverträge rechtswidrig. Falls der Vermieter eine gewisse Konstanz in der Besetzung seiner Mietwohnungen anstrebt, so hat er die Möglichkeit, durch Befristung des Mietverhältnisses eine gewisse Mindestlänge zu gewährleisten.

Soweit Wohnungsbaugesellschaften *Kontingente* einhalten müssen, etwa *für Asylbewerber* oder *Aussiedler*, ist eine entsprechende Abfrage im Fragebogen ausnahmsweise rechtmäßig.

Informationen über Einrichtungsgegenstände (z.B. Fernsehen und die Frage der Eigentumsverhältnisse) dürfen nicht abgefragt werden. Durch diese Datenerhebung will sich der Vermieter darüber informieren, an welchen eingebrachten Sachen er im Falle eines Mietrückstandes ein Vermieterpfandrecht gemäß § 559 BGB erwerben würde. Zu einem so frühen Zeitpunkt (vor Abschluß des Mietvertrages!) ist die Frage nach möglichen Pfandgegenständen unverhältnismäßig (zumal Vermieter in der Regel eine Kaution fordern).

Die Frage nach *Haustieren* ist nur zulässig, soweit deren Haltung verboten werden kann. Dies ist nach der Rechtsprechung insbesondere bei Hunden, nicht aber bei Kleintieren wie Katzen, Vögeln oder Zierfischen der Fall. Wenn die Haltung generell verboten ist, erübrigt sich die Frage, weil sie unterstellt, der Mieter werde sich über das Verbot hinwegsetzen. Nur wenn eine Wohnungsbaugesellschaft in einzelnen Häusern Haustiere in der Hausordnung verbietet, in anderen aber zuläßt, ist die Frage nach der Haltung von Haustieren zulässig.

Die Frage nach dem monatlich zur *Verfügung stehenden Geldbetrag* ist datenschutzrechtlich nicht zu beanstanden. Durch diese Frage informiert sich der Vermieter, ob der Wohnungsbewerber über eine ausreichende Bonität für die gewünschte Wohnung verfügt. Bei Wohnungsinteressenten ist allerdings auf eine genaue Aufgliederung des verfügbaren Einkommens (Ratenzahlung, Teilrente etc.) zu verzichten. Für den Vermieter ist nur von Bedeutung, daß der Mieter über ausreichendes Einkommen verfügt, nicht jedoch, wie sich das Einkommen zusammensetzt.

Insbesondere ist die Frage nach dem *Beruf* oder nach einem konkreten *Arbeitgeber* rechtswidrig. Es besteht kein Sicherungsbedürfnis des Vermieters dahingehend, daß der Mieter an einem bestimmten Arbeitsplatz seinen Lebensunterhalt verdient[56]. Insofern besteht auch keine Pflicht des Mieters mitzuteilen, wo er angestellt ist.

Bei der *Datenerhebung von Mitmietern* ist zu beachten, daß diese grundsätzlich beim jeweiligen Betroffenen erhoben werden sollten. Bei Untermietern und sonstigen Mitbewohnern ist zu beachten, daß die Vermieter anders als bei Mitmietern keinen Anspruch auf Mietzahlungen gegenüber diesen Personen haben und deshalb auch keine Informationen über das verfügbare Monatseinkommen benötigen.

Auch sollten zu sehr ins Detail gehende Angaben zu Familienangehörigen nicht gefordert werden. So hat der Vermieter kein rechtliches Interesse daran, zu erfahren, ob sein Mieter mit seiner Schwester, seiner Ehefrau, seiner Verlobten oder seiner Freundin zusammenlebt.

Der Verband Berlin-Brandenburgischer Wohnungsunternehmer hat inzwischen unserer rechtlicher Bewertung zugestimmt.

3.4 Die Kryptodebatte

Das Problem ist seit alten Zeiten bekannt: Will man Informationen oder Nachrichten geheimhalten, kann man jedoch nicht sicherstellen, daß Unbefugte sich dieser Informationen oder Nachrichten bemächtigen, so muß man sie in einer Form darstellen, mit der der Unbefugte nichts anfangen kann, der Befugte jedoch die Information oder Nachricht uneingeschränkt nutzen kann.

Das alte Problem war Jahrhunderte lang eine Domäne des geheimen Wesens, sei es der Nachrichtendienste, der geheimen Diplomatie, der militärischen Aufklärung oder der Gegenaufklärung. Angesichts des sich mit dem informationstechnischen Fortschritt auf alle Bereiche ausbreitenden Bedürfnisses, große Datenmengen über Datennetze zu übertragen, ist die Kryptographie stark in den Vordergrund des Interesses geraten. Mit der allgemeinen Verfügbarkeit kryptographischer Verfahren und den starken Anreizen zu ihrer Nutzung ist weltweit eine rechtspolitische Diskussion zur Regulierung kryptographischer Verfahren entstanden, die dabei ist, gesellschaftspolitische Dimension anzunehmen.

Für die vertrauliche Übertragung oder Speicherung von Daten gibt es grundsätzlich zwei völlig unterschiedliche Lösungsansätze: Die Steganographie und die *Kryptographie*.

Bei der *Steganographie* werden Informationen oder Nachrichten verborgen. Klassisch sind technische Mittel wie unsichtbare Tinte, doppelte Böden oder Microdots – die Nachricht im i-Punkt. Wichtiger für die aktuelle Debatte ist das Verstecken in anderen – nicht zu verbergenden – Informationen oder Nachrichten. Dafür gibt es viele Beispiele aus der Geschichte des tatsächlichen oder den Geschichten über das erfundene Geheimwesen. Sie macht es möglich, vertrauliche Daten in einem Strom von nicht vertraulichen Daten, z.B. in digitalisierten Video- oder Fernsehbildern, so zu verstecken, daß einem unbefugten Dritten die Daten unbemerkt bleiben, wenn er den Datenstrom abhört.

Bei der *Kryptographie* werden die Informationen oder Nachrichten nicht versteckt, sondern so verändert, daß sie für den Unbefugten unlesbar und unverständlich bleiben. Auch kryptographische Verfahren sind seit der Antike bekannt. Für die Ver-

[56] Amtsgericht Stuttgart, WM 1986, 331

schlüsselung und Entschlüsselung wird jeweils ein Schlüsseltext benötigt. Sender und Empfänger müssen über die passenden Schlüssel verfügen. Angreifer, die unbefugt mithören wollen, müssen sich in den Besitz des zur Entschlüsselung notwendigen Schlüssels bringen. Abgesehen davon, daß Leichtfertigkeiten dazu führen können, daß solche Schlüssel Dritten bekannt werden, steht der Angreifer vor dem Problem, den Schlüssel etwa aus dem verschlüsselten Text zu ermitteln, dem Problem der *Kryptoanalyse*. Die Stärke eines kryptographischen Verfahrens mißt sich also daran, wieviel Widerstand es Versuchen der Kryptoanalyse bieten kann. Beim Einsatz der modernen Informationstechnik erweisen sich alle aus früheren Zeiten bekannten Verschlüsselungsmethoden als unzureichend. Deshalb wurden neue Verfahren entwickelt, die ihrerseits die Potentiale moderner Informationstechnik ausnutzen und der Kryptoanalyse widersprechen.

Zu unterscheiden ist ferner zwischen *symmetrischen* und *asymmetrischen* Verschlüsselungsverfahren.

Bei *symmetrischen Verfahren* werden für die Verschlüsselung und die Entschlüsselung dieselben Schlüssel verwendet. Derjenige, der verschlüsselt, und derjenige, der entschlüsselt, müssen sich also gegenseitig den Schlüssel bekanntgegeben haben. Wenn es nur einen begrenzten Kreis von Kommunikationspartnern gibt, ist es einfach, sich von vornherein über Schlüssel zu verständigen. Ist der Kreis nicht begrenzbar, so müssen Verfahren der Schlüsselgenerierung und -verteilung gefunden werden, die bei Bedarf die an der Kommunikation Beteiligten mit den nötigen Schlüsseln versorgen. Diese Bereitstellung von Schlüsseln muß ihrerseits so vertraulich geschehen, daß Dritte dies nicht aufdecken können. Der bekannteste symmetrische Verschlüsselungsalgorithmus ist der DES-Algorithmus, der z.B. im Bankenverkehr verwendet wird.

Beim *asymmetrischen* Verfahren werden für die Verschlüsselung und die Entschlüsselung zwei verschiedene Schlüssel verwendet. Das Schlüsselpaar besteht aus einem öffentlichen und einem geheimen Schlüssel. Zur Verschlüsselung wird der öffentliche Schlüssel des Empfängers benutzt, der allein in der Lage ist, mit seinem geheimen Schlüssel die Daten zu entschlüsseln. Bei diesem Verfahren entfällt die Notwendigkeit des Schlüsselaustausches. In diese Gruppe gehören der im Internet abrufbare PGP-Algorithmus („pretty good privacy") sowie der RSA-Algorithmus.[57] Die Verfahren basieren auf der prinzipiellen Unmöglichkeit, das Produkt zweier sehr großer Primzahlen im zeitlich vernünftigen Rahmen in seine Faktoren zu zerlegen. Da Primzahlen beliebig groß sein können, kann auch die Schlüssellänge nach oben variiert werden. Das Hauptproblem besteht darin, daß die Verschlüsselung des gleichen Textes etwa 100-1000 mal mehr Rechenaufwand erfordert als z.B. DES. Ein weiteres Grundsatzproblem besteht darin, daß niemand vorhersagen kann, ob die mathematische Forschung nicht Verfahren zur Primfaktorenzerlegung entdecken wird. Dann würden alle Sicherheitssysteme, die auf dem Algorithmus aufbauen, zusammenbrechen.

Eine wichtige Anwendungsform asymmetrischer Verfahren ist die digitale Signatur. Ein zu unterschreibender Text bzw. ein Teil davon wird mit dem eigenen geheimen Schlüssel verschlüsselt und das Chiffrat mit dem Klartext mitgesendet. Der Empfänger kann mit dem öffentlichen Schlüssel des Absenders prüfen, ob die Verschlüsselung mit dem privaten Schlüssel des Absenders verschlüsselt wurde.[58] Mit einem asymmetrischen

[57] RSA = Rivest, Shamir, Adleman. Der Algorithmus ist nach den Namen seiner Entwickler benannt

[58] vgl. unten 4.7.1

Verfahren läßt sich auch eine Methode zum Schlüsselmanagement bei symmetrischen Verfahren gewinnen: Dem symmetrisch verschlüsselten Text wird der asymmetrisch verschlüsselte Schlüssel beigegeben.

Weiter wird unterschieden zwischen *geheimen* und *offengelegten* Methoden. Bei geheimen Methoden wird der Verschlüsselungsalgorithmus von den Entwicklern (Herstellerfirmen) oder bestimmten Anwendern (z.B. Sicherheitsbehörden, IT-Sicherheitsbehörden, Geheimdienste) geheimgehalten. Die Vorteile liegen darin, daß die Kryptoanalyse erschwert wird, wenn das Verfahren nicht bekannt ist, die Nachteile darin, daß diejenigen Nutzer, die das Verfahren anwenden, aber nicht kennen, sich blind darauf verlassen müssen, daß diejenigen, denen das Verfahren bekannt ist, nicht versuchen werden, ihren Informationsvorsprung für eine unbefugte Kryptoanalyse zu nutzen. Es ist ferner nicht gewährleistet, daß die Urheber der Verfahren keine Möglichkeiten vorgesehen und eingebaut haben, sich selbst Vorteile dadurch zu verschaffen, daß ihnen die Entschlüsselung leichtgemacht wird. Dieser Makel lastet auch auf heute populären Verschlüsselungsprogrammen. So sind vom DES-Algorithmus nicht alle Einzelheiten offengelegt, selbst das im Internet verbreitete PGP-Verfahren ist nicht völlig bekannt.

Diese Unwägbarkeiten gibt es bei offengelegten Methoden nicht. Hier basiert die Geheimhaltung des zu verschlüsselnden Textes allein auf der Geheimhaltung der Schlüssel. Mit der Veröffentlichung stellen sich die Algorithmen weltweiten wissenschaftlichen Untersuchungen zur Entdeckung von Schwachstellen. Verfahren, die diesen Untersuchungen standhalten, verdienen dann das Vertrauen der Anwender mehr als solche, bei denen geheimgehaltene Teile Mißtrauen erwecken.

Des weiteren unterscheiden sich kryptographische Verfahren in ihrer Stärke. Die Stärke eines kryptographischen Verfahrens mißt sich daran, wieviel Widerstand es Versuchen der Kryptoanalyse bieten kann. Für solche Kryptoanalysen werden im wesentlichen zwei Methoden verwendet: Entweder versucht ein Angreifer, den geheimzuhaltenden Schlüssel anhand eines ihm vorliegenden verschlüsselten Textes zu errechnen, oder er versucht, mit Hilfe eines Computers so lange alle Schlüssel systematisch auszuprobieren, bis er zum Erfolg kommt.

Der lange Zeit als stark geltende DES-Algorithmus gilt heute für die Übertragung hochsensibler Daten, für die unbefugte Dritte ein großes Interesse entwickeln könnten, als zu schwach, weil sein Schlüssel nur 56 binäre Zeichen lang ist. Schnellen Rechnern ist damit eine Kryptoanalyse mittels Erprobung aller möglichen Schlüssel mit nicht allzu langen Rechenzeiten möglich. Deshalb wird heute empfohlen, in solchen Fällen den sog. Triple-DES (3-DES) zu verwenden, der mit doppelter oder gar dreifacher Schlüssellänge arbeitet.

Solchen Beschränkungen unterliegen die bekannten asymmetrischen Verfahren jedoch nicht. Da das Produkt zweier Primzahlen beim RSA-Verfahren beliebig groß sein kann, kann auch die Schlüssellänge beliebig nach oben variiert werden. Allerdings besteht das Grundsatzproblem, daß niemand vorhersagen kann, ob die mathematische Forschung nicht hinreichend schnelle Verfahren zur Primfaktorenzerlegung entdecken wird. Dann würde das als sehr stark geltende RSA-Verfahren plötzlich sehr schwach werden und alle Sicherheitssysteme, die auf dem Algorithmus aufbauen, würden zusammenbrechen.

Kryptographische Methoden und Datenschutz

Die kryptographische Verschlüsselung stellt eine der wichtigsten Grundtechniken zur Herstellung informationstechnischer Sicherheit und zur Umsetzung der technisch-organisatorischen

Kontrollanforderungen der Datenschutzgesetze dar:

Sie ist obligatorisch zur Sicherstellung der *Transportkontrolle* bei der Übertragung von personenbezogenen Daten, wenn die Übertragungswege nicht der ständigen physischen Kontrolle der für die Übertragung verantwortlichen Stelle unterliegen. Davon kann in der Regel in gebäudeinternen Netzen ausgegangen werden, nicht jedoch, wenn der Datenfluß darüber hinausgeht. Die Benutzung von öffentlichen Datenübertragungswegen macht bei allen nicht-offenkundigen personenbezogenen Daten die kryptographische Verschlüsselung erforderlich, denn dies ist dann angemessen und dem technischen Stand entsprechend.

Dringend anzuraten ist die kryptographische Verschlüsselung bei der Weitergabe personenbezogener Daten auf beweglichen Datenträgern, z.B. Disketten (Datenträgeraustausch). Man kann sich dann kostspielige Sicherungen auf dem Transportweg ersparen, z.B. Disketten als Briefe statt als Wertbriefe versenden. Dies ist auch sinnvoll für die *Datenträgerkontrolle*, denn Datenträger mit verschlüsselten Daten bedürfen nicht mehr der starken Sicherung gegen Entwendung.

Sie ist ferner obligatorisch zur Sicherstellung der *Speicherkontrolle* bei allen Systemen, die nicht hinreichend gegen Diebstahl gesichert werden können. Dies gilt in vielen Fällen für Personalcomputer, stets jedoch für mobile Computer, die auch im mobilen Einsatz benutzt werden. Auch hier ist es grundsätzlich geboten, daß nicht-offenkundige personenbezogene Daten auf der Festplatte des mobilen Rechners kryptographisch verschlüsselt abgelegt werden.

In vielen andern Fällen ist der Einsatz kryptographischer Verfahren eine denkbare, in der Regel hochwirksame Alternative zu anderen üblichen Verfahren, etwa bei der maschinellen Authentifikation zwischen mehreren informationstechnischen Systemen sowie im Rahmen der *Zugangs-*, *Benutzer-*, *Speicher-* und *Zugriffskontrolle.*

In der Berliner Verwaltung haben wir insbesondere in den Fällen, in denen die Nutzung kryptographischer Verfahren als obligatorisch gelten muß, entsprechende Anforderungen gestellt. Insbesondere gilt dies für die Nutzung des Berliner Landesnetzes (bzw. MAN) zur Übertragung personenbezogener Daten.[59].

Zur Sicherung sensibler Daten und Kommunikationen über das Backbone des Verwaltungsnetzes wird vom Landesamt für Informationstechnik die VPN-Technologie empfohlen. Eine entsprechende Produktempfehlung wurde im Zusammenhang mit der Firewall-Technologie ausgesprochen.

Die Kryptoregulierung – Sicherheit durch Unsicherheit oder Unsicherheit durch Sicherheit?

Wenn Informationen auf Kommunikationsnetzen verschlüsselt werden, damit unbefugte Dritte sie nicht verstehen können, werden auch Stellen ausgeschlossen, die eine Befugnis haben, Kommunikation mitzuhören. Dies sind Sicherheits- und Strafverfolgungsbehörden, die nach der Strafprozeßordnung oder dem G 10-Gesetz den Anspruch haben, unter bestimmten, gesetzlich festgelegten Umständen Beschränkungen des Fernmeldegeheimnisses nutzen zu können. Daher erheben Sicherheits- und Strafverfolgungsbehörden weltweit die Forderung, die Nutzung kryptographischer Verfahren so zu regulieren, daß ihnen der Zugang auf den Klartext der übertragenen Daten bei Bedarf ermöglicht wird.

Dabei gibt es unterschiedliche Wege:

Das Anbieten von Verschlüsselungsdienstleistungen, das Inverkehrbringen von Verschlüsselungssystemen und die Nutzung bestimmter kryptographischer Verfahren kann verboten oder an enge Genehmigungspflichten gebunden werden. Dabei wird die Genehmigung entweder von der Vertrauenswürdigkeit der

[59] vgl. unten 4.8.1

Kommunikationspartner oder von der Möglichkeit der Behörden, den Datenfluß bei Bedarf entschlüsseln zu können, abhängen. In der Praxis bedeutet dies, daß den Sicherheitsbehörden entweder bei Bedarf ein Zugriff auf die Schlüsselinformationen gewährt wird oder der Teilschlüssel hinterlegt wird, mit dessen Hilfe die Kryptoanalyse der restlichen Schlüssel ohne Verzögerung möglich ist.

Obwohl bei Datenschützern und IT-Sicherheitsexperten seit einiger Zeit eine intensive Diskussion über mögliche Formen der Kryptoregulierung eingesetzt hat, werden in der Bundesregierung solche Fragen geradezu konspirativ angegangen. Eine aus verschiedenen Bundesministerien zusammengesetzte Arbeitsgruppe („Task Force") befaßt sich mit den Optionen für ein Kryptographiegesetz, und es wird deutlich, daß wirtschaftspolitische Gründe gegen restriktive Regelungen sprechen, sicherheitspolitische Gründe dagegen für eine strenge Reglementierung herangezogen werden.

Eine restriktive Regulierung führt nicht zu mehr öffentlicher Sicherheit, auch nicht zur Abwehr der organisierten Kriminalität.

Eine Reglementierung derart, daß nur bestimmte zugelassene kryptographische Verfahren benutzt werden dürfen, läßt sich nochmals unterlaufen, daß die Daten vor der Nutzung eines zugelassenen Verfahrens mit einem nicht zugelassenen Verfahren verschlüsselt werden (Überschlüsselung). Wer dies technisch leisten kann, bleibt also von der Kryptoregulierung unbehelligt – im Zweifel die organisierte Kriminalität, gegen die sich die Regulierung gerade richten soll.

Wer die Kryptographie zur vertraulichen Übertragung von Daten wegen der Kryptoregulierung nicht nutzen kann, dem bleibt die Steganographie. Damit können geheime Nachrichten so im Datenstrom versteckt werden, daß überhaupt nicht erkennbar ist, daß es solche Nachrichten gibt. Auch wer dies technisch leisten kann, bleibt von der Kryptoregulierung unbehelligt.

Schließlich verschafft man der Kriminalität neue Betätigungsfelder, indem man ihr ermöglicht, die wegen der Regulierung unverschlüsselt oder schwach verschlüsselt übertragenen Daten für die eigenen Zwecke zu nutzen.

Aus all dem ergibt sich, daß die Sicherheitsziele kaum durch eine restriktive Regulierung der Kryptographie erreicht werden können. Weniger Sicherheit der Vertraulichkeit der Datenübertragung führt nicht zu mehr Sicherheit für den Bürger, insbesondere nicht, wenn man die Gefahren der organisierten Kriminalität im Auge hat. Eine Kryptoregulierung wäre also verfassungsrechtlich bedenklich, weil mit erheblichem Aufwand Beschränkungen von Bürgerrechten zur unbeobachteten Kommunikation verfügt werden, ohne daß die postulierten Verbesserungen für die Sicherheit der Bürger erreicht werden können.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung zu den Eingriffsbefugnissen zur Strafverfolgung im Informations- und Telekommunikationsbereich hierzu folgende Aussage getroffen: „Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen – insbesondere im weltweiten Datenverkehr –

Die Frage, ob in welcher Weise im Interesse der Aufgabenerfüllung von Sicherheits- und Strafverfolgungsbehörden der Einsatz von Verschlüsselungstechniken geregelt werden soll, wird gegenwärtig innerhalb der Bundesregierung diskutiert. Die Bundesländer – so auch das Land Berlin – sind in diesen Prozeß eingebunden, der möglicherweise in den Entwurf eines (Bundes-)Kryptographiegesetzes münden wird. Das gewählte Verfahren ist in keiner Hinsicht ungewöhnlich, sondern folgt den üblichen Regeln einer möglichst weitgehenden politischen Klärung im Vorfeld gesetzgeberischer Initiativen. Die Behauptung, die Bundesregierung ginge diese Thematik „geradezu konspirativ" an, ist daher falsch und muß zurückgewiesen werden.

In der Sache selbst erübrigt sich eine Stellungnahme des Senats, da Diskussionsprozesse über die Notwendigkeit und den Inhalt eines Bundesgesetzes den Aufgabenkreis des Berliner Datenschutzbeauftragten nicht berühren.

Bei den derzeitigen Beratungen über die Auswirkungen fortschreitender Kryptierung geht es zunächst um Fragen der Umsetzbarkeit möglicher Verbote bzw. Genehmigungsvorbehalte gegenüber kryptographischen Verfahren auf nationaler wie auf internationaler Ebene. Der Einschätzung des Datenschutzbeauftragten, daß gerade in diesem Bereich die Umgehungsmöglichkeiten ordnungsrechtlicher Maßnahmen besonders groß sind, ist zuzustimmen. Dennoch wird nach Lösungen gesucht, die Beschränkungen der Strafverfolgung möglichst gering zu halten.

Der Senat teilt die Auffassung, daß der Ertrag für die Sicherheit von Staat und Bürgern in einem angemessenen Verhältnis zu den mit entsprechenden Maßnahmen verbundenen Einschränkungen der freien und ungestörten Kommunikation stehen muß. Es bleibt jedoch zunächst abzuwarten, welche konkreten Vorschläge unterbreitet werden.

ohnehin leicht zu umgehen und kaum kontrollierbar wären."[60]

4. Aus den einzelnen Arbeitsgebieten

4.1 Mehr Sicherheit durch Informationsverarbeitung?

4.1.1 Polizei

EUROPOL

Seit fast zwei Jahren befindet sich der Entwurf eines Bundeskriminalamtsgesetzes in parlamentarischer Beratung, das wesentliche Aspekte des Informationsverbundes der Polizeien des Bundes und der Länder regeln soll[61]. Die endgültige Fassung kann nicht unbeeinflußt bleiben von dem Übereinkommen über die Errichtung eines europäischen Polizeiamtes (EUROPOL-Konvention)[62], zu dessen Umsetzung das Bundesinnenministerium einen Gesetzentwurf vorgelegt hat.

Der Entwurf läßt deutliche Tendenzen erkennen, datenschutzrechtliche Kompetenzen zu Lasten der Länder auf den Bund zu verlagern.

Zwar wird in dem Entwurf festgestellt, daß die innerstaatlich eingebende oder übermittelnde Stelle – in der Regel die zuständige Landespolizeibehörde – die *datenschutzrechtliche Verantwortung* für den entsprechenden Datenbestand im Informations- oder Analysesystem bei EUROPOL trägt. Nicht klar definiert ist jedoch, welche datenschutzrechtliche Verantwortung parallel dazu das BKA als Zentralstelle haben soll. Zu weit geht, daß allein das Bundeskriminalamt (BKA) zur Entgegennahme von Auskunftsanträgen Betroffener befugt sein soll.

Der Bundesbeauftragte für den Datenschutz wird zutreffend als *nationale Kontrollinstanz* benannt, soweit es um die Kontrolle des BKA als nationaler Zentralstelle geht. Unberührt muß davon jedoch die Zuständigkeit der Landesbeauftragten für die Datenschutzkontrolle in den Ländern bleiben. Dies sollte im Entwurf deutlich zum Ausdruck gebracht werden. Die Regelung, wonach der Bundesbeauftragte allein das Stimmrecht in der gemeinsamen Kontrollinstanz nach Art. 24 Abs. 1 der EUROPOL-Konvention ausübt, ist nicht tragbar. Soweit die Tätigkeit der gemeinsamen Kontrollinstanz Interessen der Länder berührt, ist die Stellungnahme des Ländervertreters maßgeblich zu berücksichtigen. Anderenfalls wären die Datenschutzbeauftragten der Länder daran gehindert, die ihnen gesetzlich zugewiesenen Aufgaben zu erfüllen.

Täterorientierte Ermittlungsarbeit

Beim Polizeipräsidenten in Berlin wurde das Programm „Täterorientierte Ermittlungsarbeit" eingeführt. Darin werden gezielt ausgesuchte Tatverdächtige einem Sondersachbearbeiter zugeordnet, der alle Ermittlungsverfahren zu der ausgewählten Zielperson bearbeitet. Die damit verbundene Abkehr von der deliktischen Zuständigkeit der Vorgangsbearbeitung soll – durch die Bündelung vorhandener Erkenntnisse zu einem bestimmten Straftäter bei einem Sachbearbeiter – zielgerichtete Ermittlungs- und Operativmaßnahmen ermöglichen.

Das Programm richtet sich gegen einen speziellen Kreis von

Ob die Meldung polizeilicher Kontakte eines Betroffenen zur

[60] vgl. Anlage 2.8
[61] BT-Drs. 13/1550; vgl. JB 1995, 5.5.1
[62] Übereinkommen vom 26. Juli 1995 aufgrund von Art. K.3 des Vertrages über die Europäische Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL-Gesetz)

Tatverdächtigen, die qualitativ und/oder quantitativ besonders aktiv sind. Voraussetzung für die Aufnahme in das Programm ist, daß gegen den Betroffenen ein Ermittlungsverfahren wegen einer Straftat von erheblicher Bedeutung (§ 17 Abs. 3 und 4 ASOG) geführt wird oder im Zeitraum der letzten fünf Jahre geführt worden ist. Auf der Grundlage einer Prognoseentscheidung muß eine Wiederholungsgefahr gegeben sein, die auf Tatsachen zu stützen ist (§ 16 Abs. 3 ASOG).

Zum Zeitpunkt der von uns durchgeführten datenschutzrechtlichen Prüfung waren 66 Personen in das Programm einbezogen. Zur Umsetzung des Programms wird in den Personendatensatz jedes Betroffenen im Informationssystem Verbrechensbekämpfung (ISVB) der Hinweis aufgenommen, eine bestimmte Dienststelle zu kontaktieren. Der Hinweis ist für jeden Mitarbeiter der Polizei sichtbar, der den Personendatensatz im ISVB – egal aus welchem Anlaß – aufruft. Der Mitarbeiter vor Ort hat – nachdem er den Hinweis zur Kenntnis genommen hat – den Grund für den Abruf des ISVB-Datensatzes der angegebenen Dienststelle mitzuteilen. Von dort wird die Meldung an den Sondersachbearbeiter weitergeleitet.

Beim Sondersachbearbeiter werden im Zusammenhang mit der Durchführung des Programms „Täterorientierte Ermittlungsarbeit" keine gesonderten Datenspeicherungen vorgenommen. Als Speichermedium dient ausschließlich die Kriminalakte, die zu dem Betroffenen geführt wird. In diese wird eine Kopie des Antrages auf Einrichtung der Berichtspflicht aufgenommen.

Ein Jahr nach Aufnahme eines Betroffenen in das Programm wird geprüft, ob die Voraussetzungen für die Maßnahme noch gegeben sind. Spätestens fünf Jahre nach dem Datum der Straftat, die zur Aufnahme des Betroffenen in das Sonderprogramm geführt hat, wird der Hinweis im ISVB gelöscht.

Das Verfahren bedeutet für den Betroffenen einen erheblichen Eingriff in sein Recht auf informationelle Selbstbestimmung. Der Eingriff wird dadurch gesteigert, daß praktisch jeder Mitarbeiter der Berliner Polizei den Hinweis auf die Sondermaßnahme im Zusammenhang mit dem Abruf des Personendatensatzes des Betroffenen zur Kenntnis nehmen kann. Eine Differenzierung danach, ob der Betroffene als Tatverdächtiger, Beschuldigter, Anzeigender oder Opfer einer Straftat in Erscheinung getreten ist, erfolgt nicht. Bereits bei der ersten Prüfung des ISVB haben wir auf das Problem hingewiesen, daß Verdächtige, Anzeigende und Geschädigte sowie andere von polizeilichen Maßnahmen Betroffene unter gleichem Datensatzaufbau in der gleichen Datei des ISVB gespeichert werden. Die Vermengung der Daten dieser unterschiedlichen Personenkreise steht einer differenzierten Zweckbindung entgegen und kann zu Fehleinschätzungen führen[63].

Angesichts der vorstehend genannten strengen Voraussetzungen für die Aufnahme eines Betroffenen in das Programm ist die Speicherung des personenbezogenen Hinweises im ISVB jedoch insgesamt als verhältnismäßig (§ 11 Abs. 2 ASOG) anzusehen. Die Meldung eines bestehenden Tatverdachtes oder Ermittlungsvorganges an den Sondersachbearbeiter ist zur Straftatenverfolgung erforderlich und – gestützt auf § 42 Abs. 1 ASOG – ebenfalls zulässig. Nicht erforderlich ist zu diesem Zweck die Meldung aller anderen polizeilichen Kontakte des

Erfüllung polizeilicher Aufgaben erforderlich ist, hat die Polizei zu beurteilen. Hier gilt ebenfalls das, was der Datenschutzbeauftragte selbst unter „Zulässige Maßnahmen" zur Sinnhaftigkeit von Datensammlungen sagt. Ob es eine für den Betroffenen weniger belastende Maßnahme gibt, die in gleicher Weise wirksam für die Aufgabenerfüllung ist, kann nur aus kriminalistischer Sicht beurteilt werden. Die dem Berliner Datenschutzbeauftragten in § 24 des Berliner Datenschutzgesetzes eingeräumten Befugnisse reichen nicht soweit, daß er eigene Bewertungen an die Stelle der Bewertungen der für eine Sachaufgabe originär zuständigen Behörde setzen und sich damit de facto zur Fachaufsichtsbehörde machen kann.

[63] JB 1984, 2.4

Betroffenen. Derartige Meldungen sind unzulässig. Sie dienen nicht der Übernahme eines Ermittlungsvorganges durch den Sondersachbearbeiter, sondern der vorsorglichen Sammlung allgemeiner Erkenntnisse über den Betroffenen auf Vorrat.

Akteneinsicht und Aktenauskunft

Mit der Senatsverwaltung für Inneres und dem Polizeipräsidenten in Berlin konnte eine grundsätzliche Übereinstimmung dahingehend erzielt werden, daß der Betroffene, der einen Antrag auf Auskunft über die zu seiner Person gespeicherten Daten gestellt hat (§ 50 Abs. 1 ASOG), in die Lage versetzt werden muß, die ihm erteilte Auskunft nachzuvollziehen.

Voraussetzung dafür ist jedoch, daß dem Antragsteller Art und Umfang der Datenspeicherung sowie Anlaß und Umstände der Datenerhebung mitgeteilt werden. Diese Kriterien gelten unabhängig davon, ob über den Betroffenen nur einige wenige oder aber eine Fülle von personenbezogenen Daten zu einer Vielzahl von unterschiedlichen Sachkomplexen gespeichert sind.

Das in § 50 ASOG geregelte Auskunfts- und Akteneinsichtsrecht des Betroffenen ist Bestandteil des Grundrechtes auf informationelle Selbstbestimmung. Danach hat der Betroffene einen grundsätzlichen Anspruch darauf zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß[64]. Das bedeutet, daß ihm alle gespeicherten Daten mitzuteilen sind, die sich auf seine Person beziehen. Der Anspruch erstreckt sich dabei grundsätzlich auch auf *Daten und Informationen Dritter* (z.B. anderer Personen = Anzeigende, Zeugen, Hinweisgeber), wenn diese mit den Daten des Betroffenen verbunden sind. So können z.B. auch die Aussagen von Zeugen vom Auskunftsanspruch berührt werden, wenn sich diese gegenüber der Polizei zu einem Sachverhalt geäußert haben, der auch den Auskunftsbegehrenden betrifft. Es handelt sich dann um *Angaben mit doppeltem Personenbezug*. Beide Beteiligte – der Zeuge und der Auskunftsbegehrende – sind Betroffene i.S.v. § 4 Abs. 1 Satz 1 BlnDSG. Die Auskunft kann nur verweigert werden, wenn für einen der Beteiligten ein Geheimhaltungsinteresse besteht, das gegenüber dem Auskunftsanspruch des anderen überwiegt.

Das Aktenauskunfts- bzw. -einsichtsrecht in § 50 ASOG dient auch dem Zweck, polizeiliches Handeln im Zusammenhang mit der Verarbeitung von personenbezogenen Daten überprüfen zu können. Die in § 48 ASOG geregelten Berichtigungs-, Löschungs- bzw. Sperrungsansprüche können nur wirksam umgesetzt werden, wenn dem Auskunftsbegehrenden zuvor *umfassend* und *für ihn nachvollziehbar* Auskunft über die zu seiner Person gespeicherten Daten gewährt wird. Bei korrekter Rechtsanwendung hat dies zur Folge, daß im Rahmen der Auskunftserteilung gemäß § 50 Abs. 1 ASOG aus jeder vorhandenen Unterlage ein Extrakt zu fertigen ist, der den Auskunftsbegehrenden auch in die Lage versetzt, die über seine Person im einzelnen gespeicherten Daten auf ihre Richtigkeit hin zu überprüfen. Häufig dürfte wegen des damit einhergehenden erheblichen Arbeitsaufwandes eine *Akteneinsicht* deutlich zweckmäßiger sein als eine Auskunft nach § 50 Abs. 6 ASOG.

Die Verkehrsverwaltung hat daraus die Konsequenzen gezogen und folgerichtig das Landeseinwohneramt gebeten, angesichts des erheblichen Verwaltungsaufwandes, der mit der Auskunftserteilung aus Führerscheinakten verbunden ist, zukünftig regelmäßig von der Möglichkeit der Akteneinsicht gemäß § 50 Abs. 6 ASOG Gebrauch zu machen.

Das vom Berliner Datenschutzbeauftragten reklamierte Recht auf Akteneinsicht gibt es gegenüber Ordnungsbehörden und der Polizei nicht.

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

Die Beschränkung auf einen Auskunftsanspruch ist wegen der Besonderheiten insbesondere der polizeilichen Aufgabenerfüllung auch zwingend geboten. Der Inhalt von Kriminalakten ist anderer Natur als der Akteninhalt in Bereichen der allgemeinen Verwaltung. In fast jeder Kriminalakte sind Daten oder Informationen enthalten, auf deren Mitteilung der Betroffene keinen Anspruch hat. Dabei handelt es sich nicht nur um Daten über andere Personen, sondern auch um Informationen über polizeiliche Arbeitsabläufe und Ermittlungsmethoden oder andere behördliche Maßnahmen oder Vorgehensweisen. Gerade bei Kriminalakten besteht die Gefahr, daß sich ein Betroffener in Kenntnis solcher Informationen auf polizeiliche Maßnahmen einstellen und diese unterlaufen könnte. Andererseits verbietet es sich aus arbeitsökonomischen und auch aus kriminaltaktischen Gründen, Kriminalakten durch Umkopieren, Schwärzen oder das Einlegen von Leerblättern so „aufzubereiten“, daß sie nur noch die zur Kenntnisnahme des Betroffenen bestimmten Informationen enthalten und zur Einsichtnahme geeignet sind. Auch dies könnte zu Rückschlüssen des Betroffenen mit der Folge der vorgenannten Gefahren führen.

Die Entscheidung der Verkehrsverwaltung, bei Auskunftsbegehren aus Führerscheinakten regelmäßig Akteneinsicht nach § 50 Abs. 6 ASOG zu gewähren, beruht auf der Tatsache, daß Führerscheinakten – anders als polizeiliche Ermittlungsakten – in der Regel weder Daten Dritter noch geheimhaltungsbedürftige Daten enthalten. Außerdem erreichen Führerscheinakten oftmals einen Umfang, der eine Auskunftserteilung nicht mehr

[64] BVerfGE 65, 1, 43

Wir haben der Polizei empfohlen, entsprechend zu verfahren. Zumindest sollte ein zweistufiges Verfahren eingeführt werden. In der ersten Stufe kann – in reduzierter Form – Auskunft über den Akteninhalt gewährt werden. In der zweiten Stufe sollte dem Betroffenen allerdings die Möglichkeit einer Akteneinsicht angeboten werden. Eine Beschränkung auf die Auskunftserteilung kommt nur in Betracht, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen Daten derart verbunden sind, daß ihre Trennung auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Die Polizei hat den Vorschlag bisher lediglich insoweit aufgegriffen, als sie zukünftig in dem Auskunftsbescheid darauf hinweisen wird, daß bei Bedarf einzelne, dem Betroffenen unverständliche Angaben anhand der Kriminalakte erläutert werden können. Akteneinsicht wird nach wie vor grundsätzlich nicht gewährt.

zweckmäßig erscheinen läßt. Dabei war der Verkehrsverwaltung bei ihrer Entscheidung bekannt, daß die Polizei die Einsicht in ihre Ermittlungsakten regelmäßig verweigert und statt dessen Auskünfte nach § 50 Abs. 1 ASOG erteilt.

Da die Gewährung von Akteneinsicht nach dem Wortlaut des § 50 Abs. 6 ASOG im Ermessen der jeweiligen Behörde steht, hält der Senat die unterschiedliche Handhabung für sachlich geboten und rechtmäßig.

Datenschutzrechtliche Kontrolle der polizeilichen Einsatzleitzentrale PELZ beim Polizeipräsidenten in Berlin

Im August 1995 wurde die neue polizeiliche Einsatzleitzentrale in Betrieb genommen. Eine erste Unterrichtung erreichte uns jedoch erst knapp zwei Wochen vor der Inbetriebnahme. Diese bestand in der Übersendung eines 31 Monate alten Pflichtenheftes und einer 20 Monate alten Softwarespezifikation, also veralteter Materialien. Eine Beratung bei der Gestaltung des Verfahrens war uns somit nicht mehr möglich.

Zweck der in § 24 Abs. 3 Satz 3 BlnDSG formulierten Forderung, den Berliner Datenschutzbeauftragten über die Einführung neuer Automationsvorhaben zu informieren, ist es, uns Gelegenheit zu geben, zu dem Verfahren Stellung zu nehmen, auf datenschutzrechtliche Defizite hinzuweisen und Empfehlungen zur datenschutzgerechten Gestaltung der Verfahren zu geben. Dies setzt jedoch voraus, daß wir rechtzeitig detailliert und mit revisionsfähigen Unterlagen unterrichtet werden. Die verspätete Unterrichtung erstaunt um so mehr, als wir bei der Durchführung des letztlich gescheiterten Vorgängerprojektes ELSY (Einsatzleitsystem) intensiv eingeschaltet waren.

Da also anders Fragen des technischen Datenschutzes nicht mehr in das Projekt eingebracht werden konnten, wurde das Verfahren einer technisch-organisatorischen Kontrolle unterzogen.

Das informationstechnische Gerüst des PELZ-Verfahrens bilden drei miteinander vernetzte *UNIX-Rechner*. Die beim Betrieb dieser Systeme festgestellten technischen und organisatorischen Mängel betreffen ausschließlich Standardfragestellungen der ordnungsgemäßen Datenverarbeitung und der informationstechnischen Sicherheit, auf die bei rechtzeitiger Unterrichtung hingewiesen worden wäre.

Als besonders problematisch stellte sich der Einsatz der Fernwartung heraus. Über eine ISDN-Schnittstelle am sog. Test- und Schulungsrechner, der auch als Ausweichrechner für die beiden Echtsysteme fungiert, erfolgt die Fernwartung durch eine externe Firma. Der *Aufbau der Verbindung* kann zwar nur von der Polizei veranlaßt werden, denn die Telekommunikationsanlage ist so konfiguriert, daß ausschließlich eine Verbindung zur externen Firma, nicht aber zu anderen Stellen aufgebaut werden kann. Dies entspricht den technisch-organisatorischen Anforderungen.

Die Aktivitäten der Fremdfirma *während der Fernwartung* wurden jedoch in keiner Weise kontrolliert, obwohl sie ausschließlich und uneingeschränkt mit den allumfassenden Zu-

griffsrechten des Systemverwalters durchgeführt wurden. Die Fremdfirma konnte daher beliebig Anwender- und Systemdateien lesen, kopieren und verändern, ohne daß diese sicherheitsrelevanten Vorgänge kontrolliert wurden. Die Übermittlung personenbezogener Daten hätte auf diese Weise nicht erkannt und daher auch nicht verhindert werden können.

Alle Systemverwalter – sowohl die für das Betriebssystem als auch die für die Datenbank – sowie weitere Mitarbeiter arbeiteten gemeinsam unter einer Kennung und verfügten damit über das *gleiche Paßwort*. Eine individuelle Einräumung von Benutzer- und Administratorrechten konnte somit nicht erfolgen. Ebensowenig konnte das System die Aktivitäten der Benutzer und Systemverwalter individuell zuordnen und protokollieren.

Es war auch nicht eindeutig bekannt, wie viele Mitarbeiter über die Paßwörter für die System- oder Datenbank-Administration verfügten. Regelungen zur *Herausgabe und Neuvergabe* der Administratoren-Paßwörter konnten ebensowenig vorgelegt werden wie eine Dokumentation über Herausgabe und Neuvergabe von Paßwörtern. Es bestand damit keine Übersicht über die vergebenen Administratorrechte.

Es gab viele Benutzerkennungen von Mitarbeitern von *Fremdfirmen*, die berechtigt waren, auf der Betriebssystem-Ebene zu arbeiten. Diese konnten also Betriebssystemkommandos absetzen und Shell-Programme entwickeln, obwohl ihre Zugriffsberechtigungen inzwischen unnötig oder zumindest fragwürdig waren. Es existierten Benutzerkennungen von Mitarbeitern des Polizeidienstes, die entweder aus dem Dienst *ausgeschieden* oder *versetzt* worden waren.

Diese zum Teil gravierenden Mängel wurden beanstandet, in der Stellungnahme wurde mitgeteilt, daß sie unseren Empfehlungen entsprechend unverzüglich beseitigt wurden. Auf eine Fernwartung soll nunmehr vollkommen verzichtet werden.

Strafverfolgung in der Informationsgesellschaft

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt dazu, daß das Kommunikationsverhalten der Bürger in bisher nicht für möglich gehaltenem Ausmaß registriert wird. Die Nutzung der neuen Medien hinterläßt zahllose *personenbezogene Datenspuren*. Nicht nur Daten über den Inhalt und Umfang der Kommunikation sind auswertbar vorhanden, sondern auch Bewegungsprofile aufgrund von Aktiv-Meldungen von Mobiltelefonen können erstellt werden. Die Telekommunikationsnetze verändern dadurch ihre Struktur und Funktion: sie können von Kommunikationsnetzen der Bürger zu Überwachungsnetzen der Sicherheitsbehörden werden[65]. Eine ähnliche Entwicklung droht im Bereich der Nutzung von Telediensten[66].

In einer Entschließung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder festgestellt, daß die herkömmlichen, weitreichenden *Eingriffsbefugnisse der Strafverfolgungsbehörden* unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können[67]. Die zum Schutz der Persönlichkeitsrechte des Einzelnen gezogenen Grenzen müssen auch unter den geänderten Bedingungen der modernen Informationstechnologie gewährleistet werden.

Von besonderer Bedeutung ist die Möglichkeit des Bürgers, wie bisher im analogen Telefonnetz spurlos zu kommunizieren.

[65] vgl. unten 4.7.1
[66] vgl. unten 4.7.2
[67] Anlage 2.8

Vorrang verdienen solche Systeme, die keine oder möglichst wenig personenbezogene Daten verarbeiten. Eine nur vorsorgliche Bereithaltung von Daten für Zwecke einer künftig denkbaren Strafverfolgung ist abzulehnen. Die Tatsache, daß die neuen Informations- und Kommunikationstechniken auch für kriminelle Zwecke genutzt werden können, rechtfertigt es nicht, alle Nutzer von vornherein einer so weitgehenden Überwachung zu unterwerfen, wie sie der bisherigen Kommunikationsinfrastruktur jedenfalls fremd war. Die vorhandenen Befugnisse der Strafverfolgungsbehörden reichen aus und müssen teilweise durch den Gesetzgeber vor dem Hintergrund der neuen Informations- und Kommunikationstechniken verfassungskonform eingeschränkt (präzisiert) werden.

Der Zugriff auf *Bestands- und Verbindungsdaten* ist insbesondere im Hinblick auf den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, amtliches Vertrauensverhältnis) und wegen der Rückschlüsse von den Verbindungsdaten auf den Inhalt der Kommunikation strikt zu beschränken.

Eine Reglementierung der Verschlüsselung, z.B. durch den Zwang zur Schlüsselhinterlegung, wird abgelehnt, da diese Maßnahme ohnehin leicht zu umgehen und selbst mit einem hohen bürokratischen Aufwand kaum effektiv zu kontrollieren wäre[68].

4.1.2 Verfassungsschutz

Sicherheitsüberprüfungen

Der *Gesetzentwurf über den Geheim- und Sabotageschutz* im Land Berlin[69] wurde noch immer nicht in das Abgeordnetenhaus eingebracht. Die mit der Sicherheitsüberprüfung verbundenen erheblichen Informationseingriffe erfolgen somit nach wie vor ohne gesetzliche Grundlage. Es ist dringend geboten, daß dieser bedeutendste Mangel der Berliner Gesetzgebung behoben wird.

Auf Bundesebene wurde inzwischen ein weiteres Gesetz mit Regelungen zur Sicherheitsüberprüfung auf den Weg gebracht. Der Gesetzentwurf der Bundesregierung und ein gleichlautender Gesetzentwurf einiger Abgeordneter der CDU und F.D.P.[70] für ein Zweites Gesetz zur Änderung des Gesetzes zu Art. 10 Grundgesetz (GG)[71] verpflichtet Unternehmen, die *Postdienstleistungen* für die Öffentlichkeit anbieten, zur Mitwirkung bei der Überwachung des Postverkehrs durch die Nachrichtendienste. Als Folge der zunehmenden Öffnung der Postdienstleistungsmärkte für private Unternehmen (z.B. für Massensendungen und Kurierdienste) sollen die bestehenden Regelungen, die die Überwachung des Postverkehrs bisher durch Mitwirkung der Deutschen Bundespost sicherstellten, an die neuen Entwicklungen angepaßt werden.

In den Gesetzentwürfen ist auch vorgesehen, daß sich Mitarbeiter dieser Unternehmen einer *Sicherheitsüberprüfung* zu unterziehen haben. Zu begrüßen ist, daß die Überprüfung erst bei einer konkreten Überwachungsmaßnahme erfolgen und auf

Der Gesetzentwurf – die Bezeichnung des Gesetzes wurde im Rahmen der Erarbeitung zwischenzeitlich in „Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Berlin (Berliner Sicherheitsüberprüfungsgesetz)“ geändert – ist vom Senat beschlossen und dem Abgeordnetenhaus zugeleitet worden..

Eine Stellungnahme zum Zweiten Gesetz zur Änderung des Gesetzes zu Art. 10 Grundgesetz erübrigt sich, da es sich um ein Bundesgesetz handelt.

68 vgl. oben 3.4
69 JB 1995, 5.1
70 BT-Drs. 13/5753
71 BR-Drs. 552/96

die Personen beschränkt werden soll, die mit der Maßnahme betraut werden sollen. Der Umfang der Überprüfung soll auf eine einfache Sicherheitsüberprüfung beschränkt werden. Die erweiterte Sicherheitsüberprüfung und die erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen, jeweils unter Einbeziehung des Ehepartners oder Lebensgefährten, sollen durch diese Gesetzesänderung entfallen. Der Bundesrat hat sich gegen diese aus datenschutzrechtlicher Sicht zu begrüßenden Regelungen gewandt und eine vorsorgliche und weitergehende Sicherheitsüberprüfung von Mitarbeitern gefordert. Darüber hinaus soll die Regelung wieder eingeführt werden, daß eine Unterrichtung des Betroffenen nach Ablauf von fünf Jahren unterbleiben soll.

Der Verzicht auf eine vorsorgliche Sicherheitsüberprüfung ist im Hinblick auf die stetig wachsende Zahl der Überwachungsmaßnahmen mitwirkungspflichtiger privater – auch mittlerer und kleiner – Unternehmen, bei denen nicht feststeht, ob sie überhaupt jemals für G 10-Maßnahmen in Anspruch genommen werden, ein Gebot der Verhältnismäßigkeit. Dies betrifft auch die Beschränkung auf die einfache Sicherheitsüberprüfung, da der Umfang der übermittelten Daten zur Durchführung der Überwachungsmaßnahme äußerst gering ist. Die Bundesregierung hat den Vorschlägen des Bundesrates deshalb zu Recht nicht zugestimmt[72]. Der Bundestag ist den Wünschen des Bundesrates nicht gefolgt und hat den von den Abgeordneten eingebrachten Gesetzentwurf, mit einigen Änderungen in für den Datenschutz nicht relevanten Punkten, so beschlossen[73].

Eingaben in NADIS

Das Nachrichtendienstliche Informationssystem NADIS wird gemeinsam von den Verfassungsschutzbehörden des Bundes und der Länder betrieben. Im Zusammenhang mit der Überarbeitung der NADIS-Richtlinien hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mehrheitlich gefordert, die im NADIS zu speichernden Daten zu verringern und die Angaben zu streichen, die nicht Identitätszwecken dienen[74]. Auch in der mit den Landesämtern für Verfassungsschutz abgestimmten Dateianordnung für die „*Personenzentraldatei*" (PZD) ist der zu speichernde Datensatz zu umfangreich. In NADIS-PZD sind Personengrunddaten, Aktenzeichen sowie einige Zusatzinformationen enthalten. Diese können von den Verfassungsschutzbehörden direkt abgerufen werden. Die Datenspeicherungen lassen erkennen, welche Verfassungsschutzbehörde noch über weitere Informationen zu dem Betroffenen verfügt.

Der vorgesehene Datenumfang widerspricht § 6 Satz 2 Bundesverfassungsschutzgesetz. Danach dürfen nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind, gespeichert werden. Die Regelung läßt nur ein reines *Aktenhinweissystem* zu. Die Datenspeicherung hat sich auf die Identitätsmerkmale einer Person zu beschränken, die zum Auffinden der zur Person gehörenden Akte erforderlich sind. Hierfür sind die Identitätsdaten des Betroffenen in der Regel ausreichend, wie sie etwa in § 111 Abs. 1 Ordnungswidrigkeitengesetz enthalten sind.

Zwar können auch andere Angaben zur Identifikation einer Person beitragen. Das allein kann jedoch die Erforderlichkeit für die Speicherung in einem Aktenhinweissystem nicht rechtfertigen. Anderenfalls könnte jede nur denkbare Angabe über eine Person mit der Argumentation, sie könne zum Auffinden von

Diese Rechtsauffassung wird durch den Senat nicht geteilt. Bei den hier strittigen Zusatzinformationen handelt es sich um Kraftfahrzeug-, Konto- und Schließfachangaben, die im Einzelfall auch zur Identifizierung einer Person und zum Auffinden von Unterlagen geeignet sein können. Im übrigen war es nicht die Absicht des Gesetzgebers, die schon vor Inkrafttreten des Bundesverfassungsschutzgesetzes übliche und nach den praktischen Erfahrungen unverzichtbare Speicherung dieser Daten einzuschränken. Aus diesem Grund hat auch der Bundesbeauftragte für den Datenschutz seine ursprünglichen Bedenken gegen diese Speicherung zurückgestellt.

Der Berliner Datenschutzbeauftragte kontrolliert die Einhaltung bundesrechtlicher Datenschutzvorschriften, die durch Landesbehörden angewandt werden. Fragen, die die Auslegung eines Bundesgesetzes betreffen (hier: § 6 Satz 2 Bundesverfassungsschutzgesetz), müssen aber auf der

[72] BR-Drs. 13/5890
[73] BR-Drs 4/97
[74] JB 1994, 4.1 und Anlage 2.7

Akten beitragen, gespeichert werden. Damit würde die vom Bundesverfassungsschutzgesetz eindeutig gezogene Grenze zwischen Aktenhinweissystemen und der sachbezogenen nachrichtendienstlichen Arbeit in Recherchedateien verwischt. Für den Bereich des gewaltfreien Extremismus hat der Gesetzgeber eine Begrenzung der Angaben auf ein reines Aktenhinweissystem vorgesehen. Diese Entscheidung kann nicht durch eine Ausdehnung des Datenbestandes in der Dateianordnung umgangen werden.

zuständigen (Bundes-) Ebene geklärt werden; dies ist hier geschehen.

Stellungnahme – ja, aber bitte nicht weiter stören

Die Senatsverwaltung für Inneres hatte uns den Entwurf einer Dateianordnung im G 10-Bereich – also der *Überwachung des Telefon- und Postverkehrs* – übersandt mit dem Hinweis, wir seien zwar nicht kontrollbefugt, es entspreche aber der bundesweiten Praxis, die Datenschutzbeauftragten formlos in das Zustimmungsverfahren einzubeziehen. Als wir dann – insbesondere zu technisch-organisatorischen Maßnahmen – nachfragten und zu den datenschutzrechtlichen Aspekten Stellung genommen hatten, erhielten wir die Mitteilung, daß die Vorschrift überarbeitet und uns die überarbeitete Fassung frühzeitig zur Stellungnahme bzw. Herstellung des Benehmens nach § 16 Landesverfassungsschutzgesetz (LfVG) vorgelegt wird. Nachdem wir an die Beantwortung unserer Fragen zu den Datensicherungsmaßnahmen erinnert hatten – die unabhängig von einer Überarbeitung der Vorschriften vorliegen müssen –, wurde uns mitgeteilt, daß wir für den gesamten Bereich des G 10-Verfahrens nicht kontrollbefugt seien und zukünftig von unserer Beteiligung abgesehen werde.

Abgesehen von dieser Verfahrensweise, die keiner weiteren Kommentierung bedarf, ist diese Auffassung auch sachlich unzutreffend.

Der Kontrolle durch den Berliner Datenschutzbeauftragten unterliegen nur personenbezogene Informationen, die nicht der Kontrolle durch die G 10-Kommission unterliegen (§ 34 Abs. 4 Satz 4 LfVG).

Die *G 10-Kommission* entscheidet lediglich über die Überwachungsmaßnahmen sowie die Unterrichtung der Betroffenen von diesen Maßnahmen (§ 2 Abs. 2 und 3 Ausführungsgesetz zum G–10 AG G 10). Sie ist über den Vollzug der Überwachungsmaßnahmen und die Unterrichtung der Betroffenen zu informieren. Hieraus folgt, daß die Kommission den Umgang mit personenbezogenen Daten nur insoweit kontrolliert, als sie über die Zulässigkeit von Überwachungsmaßnahmen und die Unterrichtung der Betroffenen zu entscheiden hat. Soweit die Kommission keinen gesetzlichen Kontrollauftrag hat, bleibt es bei der Kontrollbefugnis des Berliner Datenschutzbeauftragten.

Die Auffassung, daß der gesamte Bereich der Post- und Telefonüberwachung nach dem G 10 nicht unserer Prüfungskompetenz unterliegt, findet in der gesetzlichen Kompetenzzuweisung keine Stütze. Dem Berliner Datenschutzbeauftragten obliegt die Kontrolle der Verarbeitung, insbesondere der Auswertung, Speicherung und Übermittlung der durch die Überwachung gewonnenen personenbezogenen Daten (soweit darüber nicht die Kommission entschieden hat), der Verarbeitung und Nutzung personenbezogener Daten im Vorfeld und zur Vorbereitung von Überwachungsmaßnahmen, der technischen und organisatorischen Maßnahmen (§ 5 BlnDSG) und die Einhaltung der Vorschriften zugunsten von Personen, über die Daten verarbeitet werden, die aber nicht Betroffene von Überwachungsmaßnahmen sind und daher durch das G 10 nicht geschützt werden. Die Aufteilung der Kontrollzuständigkeiten entspricht im übrigen der Vorstellung des Bundesverfassungsgerichtes, das in seiner

Zwischen dem Berliner Datenschutzbeauftragten und der Senatsverwaltung für Inneres wurde im Rahmen eines Schriftwechsels das Für und Wider in der Sache hinreichend erörtert.

Die Ausführungen des Berliner Datenschutzbeauftragten zur Zuständigkeit stimmen mit der Rechtsauffassung des Senats nicht überein:

Das Gesetz räumt in § 31 Abs. 4 Satz 4 LfVG der G 10-Kommission des Landes Berlin ein umfassendes Kontrollrecht ein, so daß der gesamte Bereich der Post- und Telefonüberwachung nach dem G 10-Gesetz nicht der Prüfkompetenz des Berliner Datenschutzbeauftragten unterliegt. Es handelt sich bei der Vorschrift um eine spezielle Regelung im Verhältnis zu den allgemeinen datenschutzrechtlichen Bestimmungen. Der G 10-Kommission steht es aber frei, den Berliner Datenschutzbeauftragten zu ersuchen, die Einhaltung der Regelungen des Datenschutzes bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren.

Entscheidung zur strategischen Postkontrolle die Kontrolle durch unabhängige und an keine Weisung gebundene, staatliche Organe und Hilfsorgane zur Bedingung verfassungsmäßiger Grundrechtseingriffe erklärt und dabei die Kommission nach dem G 10 und die Datenschutzbeauftragten gleichberechtigt nebeneinandergestellt hat[75].

Im übrigen ist die Feststellung der Senatsverwaltung für Inneres, daß die Kontrolle der Datenverarbeitung sich nicht von der Kontrolle der verarbeiteten Daten trennen läßt, sachlich falsch. Bei allen Kontrollen der Ordnungsmäßigkeit (§ 19 Abs. 1 BlnDSG) und Sicherheit der Datenverarbeitung (§ 5 Abs. 3 BlnDSG), die der Berliner Datenschutzbeauftragte durchführt, ist der Zugriff auf die Daten nicht erforderlich.

Neues Verfassungsschutzgesetz ohne Auswirkungen

Es ist zu begrüßen, daß das Landesamt für Verfassungsschutz durch einen *Arbeitsplan* die Verwendung personenbezogener Daten genauer festgelegt hat und damit für eine einheitliche und transparente Verfahrensweise sorgt. Es würde möglicherweise den unterschiedlichen Aufgaben noch besser Rechnung tragen, wenn – wie z.B. bei dem Bundesamt für Verfassungsschutz – für die Bereiche Extremismus, Sicherheitsüberprüfung, Ausländerextremismus und Spionageabwehr differenzierte Arbeitspläne erstellt würden.

Der Arbeitsplan betrifft ausschließlich die Speicherungen zum Zwecke der Extremismusbeobachtung und der Spionageabwehr. Für den Bereich der Sicherheitsüberprüfungen gelten besondere Regelungen.

In dem Arbeitsplan wird insbesondere festgelegt, welche personenbezogenen Daten für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz zu erfassen und nach welchen Fristen sie zu überprüfen sind. Diese Regelungen sind von besonderer Bedeutung für die Beachtung des Persönlichkeitsrechtes der Betroffenen. Hierbei sind der Verhältnismäßigkeitsgrundsatz und die im Gesetz über das Landesamt für Verfassungsschutz (LfVG) vorgesehenen Beschränkungen zu beachten. Der Festlegung der betroffenen Personenkreise kommt dabei besondere Bedeutung zu. Es muß sichergestellt sein, daß nur Aktivitäten und Verhaltensweisen von einigem Gewicht zu einer Erfassung beim Verfassungsschutz führen können.

Aus diesem Grund hat der Gesetzgeber die Grenze zum verfassungsschutzrelevanten Verhalten festgelegt: Nach § 6 Abs. 1 Satz 2 LfVG ist menschliches Verhalten nur verfassungsschutzrelevant, soweit der Betroffene einen extremistischen Personenzusammenschluß *nachdrücklich* unterstützt. Einfache Mitglieder und Anhänger werden davon nicht erfaßt. Sie dürfen nur beim Verfassungsschutz registriert werden, wenn weitergehende Aktivitäten feststellbar sind.

§ 6 Abs. 1 Satz 2 LfVG fordert, soweit das Verhalten von Einzelpersonen im Hinblick auf einen Personenzusammenschluß betroffen ist, eine nachdrückliche Unterstützung dieses Zusammenschlusses. Die Folgerung des Berliner Datenschutzbeauftragten, daß daher einfache Mitglieder nicht erfaßt werden dürften, ist in dieser Allgemeinheit aber nicht zutreffend. Nach § 7 Abs. 1 in Verbindung mit § 6 Abs. 1 Satz 2 LfVG darf das Landesamt für Verfassungsschutz tätig werden, wenn tatsächliche Anhaltspunkte für den Verdacht der nachdrücklichen Unterstützung einer extremistischen Bestrebung bestehen. Derartige Anhaltspunkte werden in aller Regel bereits durch die Mitgliedschaft in einem vom Landesamt für Verfassungsschutz beobachteten Personenzusammenschluß begründet.

Das Landesamt für Verfassungsschutz hält dagegen eine *Registrierung einfacher Mitglieder* ohne weitere Voraussetzung für zulässig[76]. Es meint, nach § 6 Abs. 1 LfVG sei zwischen dem Handeln *in* einem und *für* einen Personenzusammenschluß zu unterscheiden. Nur bei einem Handeln *für* einen Personenzusammenschluß sei eine nachdrückliche Unterstützung erforderlich. Eine Konkretisierung der Eingriffsschwelle beim Handeln *in* einem Personenzusammenschluß sei nicht erforderlich, da hier bereits die formale Mitgliedschaft eine nachdrückliche Unterstützung bedeute.

Wir teilen diese Auffassung nicht. Der Landesgesetzgeber hat sich – im Gegensatz zu anderen Regelungen – bei § 6 Abs. 1 LfVG bewußt für eine vom Bundesverfassungsschutzgesetz abweichende Regelung entschieden. Zwar können Organisatio-

[75] BVerfGE 67, 157, 183

[76] Stellungnahme des Senats zu unserem JB 1995, Drs. 13/595

nen nur durch die ihr angehörenden Personen handeln, daraus folgt jedoch für den Bereich des gewaltfreien Extremismus nicht, daß die Daten eines jeden einzelnen Mitgliedes vom Verfassungsschutz erhoben und gespeichert werden dürfen. Für diesen Eingriff bedarf es einer höheren Eingriffsschwelle, die in § 6 Abs. 1 Satz 2 LfVG normiert ist: die nachdrückliche Unterstützung.

Einmal in den Akten, immer in den Akten

Ein Bürger beschwerte sich bei uns über seine Registrierung beim Landesamt für Verfassungsschutz. Das Landesamt hatte seine Daten in das bundesweite Nachrichtendienstliche Informationssystem (NADIS) eingegeben. Hintergrund war seine vorläufige Festnahme anläßlich einer Demonstration vor einigen Jahren.

Die Polizei hatte eine Liste mit Personen übermittelt, die bei einer *Demonstration vorläufig festgenommen* wurden. Ungeachtet unserer grundsätzlichen Bedenken gegen die Übermittlung und Speicherung derartiger Personenlisten[77] haben wir die sofortige Löschung der Daten des Petenten gefordert, da über ihn keine weiteren Erkenntnisse vorlagen, die Umstände der Festnahme nicht bekannt waren und eine Einstellung des Verfahrens gegen ihn erfolgt war. Bei dieser Sachlage ist eine weitere Speicherung der Daten des Petenten – auch wenn dies nur noch für einige Monate vorgesehen war – im NADIS unverhältnismäßig.

Das Landesamt für Verfassungsschutz erklärte sich bereit, die Daten des Petenten im NADIS sofort zu löschen. Auch bei weiteren 39 Personen wurde eine Löschung der Daten veranlaßt, und bei 63 Personen, die zum Zeitpunkt der Festnahme nicht in Berlin gemeldet waren, wurden die Daten auf der Liste geschwärzt, weil diese für die Aufgabenerfüllung des Verfassungsschutzes nicht relevant waren. Weiterhin wurde mitgeteilt, daß nunmehr die gesamte Liste vernichtet wird und alle hierauf beruhenden Speicherungen in Dateien gelöscht werden.

Einige Monate später teilte das Landesamt für Verfassungsschutz mit, daß die Liste vernichtet worden sei, aber erneut angefordert wurde. Die Daten der darin registrierten Personen, die für die Arbeit des Verfassungsschutzes nicht relevant sind, seien gesperrt worden. Eine Schwärzung der Daten dieser Personen wurde abgelehnt, da wegen des aufgrund der Sperrung bestehenden Nutzungs- und Übermittlungsverbotes praktische Konsequenzen für die Betroffenen ausgeschlossen seien.

Das Vorgehen des Landesamtes für Verfassungsschutz verstößt gegen § 27 Abs. 2 LfVG. Durch Anforderung der kompletten Personenliste wurden bewußt auch Daten von Personen angefordert, die für die Aufgaben des Verfassungsschutzes irrelevant sind. Der Hinweis des Landesamtes für Verfassungsschutz, daß nach einer Übermittlung der nicht erforderlichen Daten nach § 27 Abs. 6 LfVG nur eine Sperrung der Daten in Betracht komme, ist vor dem Hintergrund, daß ursprünglich eine Löschung der Daten der Betroffenen auch in den Unterlagen zugesagt wurde und auf der ursprünglichen Liste auch eine Schwärzung von Daten bereits erfolgt war, unverständlich.

Auch die Speicherung gesperrter personenbezogener Daten in Akten des Verfassungsschutzes ist ein Eingriff in das Persönlichkeitsrecht der Betroffenen und wird – wie Eingaben von Bürgern immer wieder zeigen – als erhebliche Belastung empfunden. Nach § 27 Abs. 6 LfVG hat das Landesamt für

Die Festnahmeliste wurde bei einer Demonstration anläßlich der Räumung der besetzten Häuser in der Mainzer Straße am 14. November 1990, bei der es zu den bisher schwersten gewalttätigen Auseinandersetzungen zwischen Autonomen und Polizeibeamten seit der Wiedervereinigung Berlins gekommen ist, erstellt. Die Informationen über die in diesem Zusammenhang erfolgten Festnahmen sind zur Bewertung des gewaltbereiten Extremismus unverzichtbar. Der Betroffene wurde wegen Verdachts des Landfriedensbruchs festgenommen und befristet im NADIS erfaßt.

Auf der Liste enthaltene nicht erforderliche Daten wurden entsprechend der üblichen Verfahrensweise zunächst als gesperrt gekennzeichnet und anläßlich der datenschutzrechtlichen Prüfung auf Anregung des Berliner Datenschutzbeauftragten geschwärzt.

Die Liste wurde auf Wunsch der Polizei vernichtet, weil es sich um eine interne Einsatzunterlage handelte, die in dieser Form nicht an das Landesamt für Verfassungsschutz übermittelt werden sollte. Eine offizielle Festnahmeliste wurde angefordert, weil die Speicherungen der relevanten Personen im NADIS ohne Aktenrückhalt hätten widerrufen werden müssen. Dies wäre angesichts der Bedeutung der Ereignisse am 14. November 1990 fachlich nicht vertretbar gewesen. Die Speicherung relevanter Personen wurde auf der Basis der neuen Liste aufrechterhalten. Der Vorwurf, das Landesamt für Verfassungsschutz habe bewußt, also vorsätzlich, Daten von Personen angefordert, ist in dieser Form nicht berechtigt. Eine Bezeichnung der nicht erforderlichen Personen bei der erneuten Anforderung der Liste wäre nicht möglich gewesen, da diese Daten bereits geschwärzt worden waren. Allerdings wurde nicht bedacht, daß im konkreten Fall ein auf die als relevant erkannten Personen begrenztes Übermittlungsersuchen hätte gestellt werden können. Diesen Mangel hat das Landesamt für Verfassungsschutz gegenüber dem Berliner Datenschutzbeauftragten bereits eingeräumt.

Die Sperrung der nicht erforderlichen Daten entspricht der beim Landesamt für Verfassungsschutz üblichen Verfahrensweise. Eine Trennung nicht benötigter Daten durch Schwärzen und Kopieren stellt einen unverhältnismäßigen Aufwand dar. Da die Erforderlichkeit der Speicherung in vielen Fällen nicht sofort, sondern erst nach weiteren Ermittlungen beurteilt werden kann und auch eine zunächst bejahte Relevanz z.B. aufgrund der Einstellung eines Ermittlungsverfahrens entfallen kann, müßte eine Festnahmeliste im Laufe ihrer u.U. sehr lange andauernden Bearbeitung so oft kopiert werden, daß die Lesbarkeit der Unterlage infrage gestellt würde.

[77] JB 1993, 4.5.2

Verfassungsschutz bei übermittelten Informationen deshalb nach ihrem Eingang unverzüglich zu prüfen, ob sie zur Erfüllung seiner Aufgaben erforderlich sind. Ist das nicht der Fall, sind die Unterlagen unverzüglich zu vernichten. Die Vernichtung darf nur unterbleiben, wenn die Trennung von anderen *Informationen*, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand erfolgen kann. Das heißt: Wenn in einer Unterlage erforderliche von nicht erforderlichen Informationen mit vertretbarem Aufwand voneinander getrennt werden können, ist die übermittelte Unterlage zu vernichten. Aufbewahrt werden darf eine gefertigte Kopie, auf der die nicht erforderlichen Daten geschwärzt sind. Durch Schwärzung und Kopieren der nicht erforderlichen Daten auf der Liste ist eine Trennung der vom Verfassungsschutz für erforderlich gehaltenen Angaben von den nicht erforderlichen Daten mit vertretbarem Aufwand möglich.

Durch die Sperrung werden Daten der Betroffenen hinreichend geschützt. Mangels Speicherung im NADIS können sie nicht gezielt gesucht und gefunden werden. Eine versehentliche Nutzung der Daten ist durch die Kennzeichnung ausgeschlossen.

4.2 Der registrierte Bürger: Ordnungsbehörden

4.2.1 Meldewesen

Jetzt auch in Berlin: GEZ überholt den Möbelwagen

Nachdem in einigen Bundesländern eine Befugnis zur regelmäßigen Übermittlung von Meldedaten an die Gebühreneinzugszentrale (GEZ) geschaffen worden war, hat auch die Senatsverwaltung für Inneres ihre ablehnende Haltung[78] zu diesem Verfahren aufgegeben und einen Entwurf zur Änderung der Verordnung zur Durchführung des Meldegesetzes (DVO-Meldegesetz) vorgelegt, weil der SFB das Verfahren für das Aufspüren von *Schwarzhörern und -sehern* nicht für ausreichend hält.

Wir haben bereits im Jahresbericht 1993 die geplante regelmäßige Datenübermittlung aus dem Melderegister an die Rundfunkanstalten bei jeder An- und Abmeldung wegen des damit verbundenen unverhältnismäßigen Eingriffs in das informationelle Selbstbestimmungsrecht abgelehnt[79]. Daran haben wir festgehalten. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich 1993 gegen dieses Verfahren ausgesprochen[80].

Gegen die Übermittlung der Daten von Schwarzhörern bestehen zwar keine Bedenken. Bei dem vorgesehenen Verfahren werden allerdings auch die Daten derjenigen übermittelt, die ihre Gebühren bezahlen oder kein Empfangsgerät besitzen oder als Familienmitglied eines Gebührenzahlers selbst nicht gebührenpflichtig sind. Die regelmäßige Übermittlung der Daten *aller* über 18jährigen ist daher nicht nur nicht erforderlich, sondern auch im Hinblick auf das informationelle Selbstbestimmungsrecht nicht mehr verhältnismäßig.

Mit der Nutzung der Meldedaten zum Zweck des Gebühreneinzuges ist eine weitere *Durchbrechung des Verwendungszweckes von Meldedaten* verbunden. Dies ist für die Durchführung öffentlicher Aufgaben im engeren Sinne (z.B. Erstellung von Lohnsteuerkarten) noch hinnehmbar, hätte aber bei einer Übermittlungsbefugnis an den SFB und die GEZ zur Folge, daß derartige Datenübermittlungen auch von anderen Stellen gefordert werden könnten, die öffentliche Aufgaben im weitesten Sinne wahrnehmen und dafür eine Gebühr erheben (z.B. GASAG, BEWAG, BSR).

Die von der Senatsverwaltung für Inneres Ende 1996 erlassene Rechtsverordnung zur Änderung der Verordnung zur Durchführung des Meldegesetzes (DVO-Meldegesetz) erlaubt es der Berliner Meldebehörde, dem SFB bzw. der von ihm beauftragten GEZ zum Zwecke der Erhebung und des Einzugs der Rundfunkgebühren im Falle der Anmeldung oder des Todes eines volljährigen Einwohners folgende seiner im Melderegister registrierten Daten einmal monatlich zu übermitteln:

1. Familienname,
2. frühere Namen,
3. Vornamen,
4. Doktorgrad,
5. Tag der Geburt,
6. gegenwärtige und letzte frühere Anschrift, Haupt- und Nebenwohnung,
7. Tag des Ein- und Auszuges,
8. Familienstand,
9. Sterbetag.

Die übermittelten Daten dürfen nur verwendet werden, um Beginn und Ende der Rundfunkgebührenpflicht sowie die Landesrundfunkanstalt, der die Gebühr zusteht, zu ermitteln. Der SFB und die von ihm beauftragte GEZ haben durch organisatorische und technische Maßnahmen sicherzustellen, daß die Kenntnisnahme nur durch berechtigte Bedienstete zur Aufgabenerfüllung erfolgt und daß nicht mehr benötigte Daten unverzüglich gelöscht werden, spätestens aber innerhalb eines halben Jahres nach ihrer Übermittlung.

Die in Berlin erlassene Regelung orientiert sich an einem von der IMK im Jahre 1993 empfohlenen Musterentwurf. In den Bundesländern Nordrhein-Westfalen, Hessen, Baden-Württemberg, Bayern und Saarland wurden entsprechende regelmäßige Datenübermittlungen an die dortigen Landesrundfunkanstalten bzw. an die GEZ bereits zugelassen. In weiteren Bundesländern wird eine Zulassung erwogen.

Bei der Abwägung, ob der Wunsch des SFB bzw. der GEZ auf Zulassung von regelmäßigen Datenübermittlungen

[78] vgl. die Antwort des Senats auf die Kleine Anfrage Nr.4619, LPD vom 15. Dezember 1993
[79] vgl. JB 1993, 5.2
[80] JB 1993, Anlage 2.3
[81] GVBl 1996, 551

Hinzu kommt, daß bei denjenigen, die ihre Gebühren korrekt bezahlen oder nicht gebührenpflichtig sind, nach dem vorliegenden Entwurf mehr Daten übermittelt werden sollen, als die Rundfunkanstalten und die GEZ nach § 3 Abs. 2 des Rundfunkgebührenstaatsvertrages bei den Betroffenen selbst erheben dürfen.

Als Alternative wurden im Abgeordnetenhaus Maßnahmen vorgeschlagen, die auch ohne regelmäßige Datenübermittlung die Bereitschaft zur rechtzeitigen Anmeldung bei der GEZ steigern. Hierzu gehört z.B., daß *GEZ-Formulare* nicht nur in den Banken, sondern *auch in den Meldestellen ausgelegt* werden

Als sich herausstellte, daß der Senat sich aus gebührenpolitischen Gründen unseren Bedenken nicht anschließen würde, schlugen wir vor, daß die meldepflichtigen Personen eine bessere Chance erhalten sollten, sich von sich aus anzumelden, bevor sie aufgrund des Datenabgleiches als potentielle Schwarzhörer und -seher eingestuft werden. Die Daten aus dem Melderegister sollten nicht sofort am Monatsende, sondern zeitverzögert *erst nach drei Monaten* übermittelt werden. Damit würden bei dem Datenabgleich nur diejenigen Personen „ausgerastert", die drei Monate lang ihrer Meldepflicht nicht nachgekommen sind. Für die Berechnung der Höhereinnahmen ergibt sich damit auch eine bessere Ausgangsbasis, da bei einem umgehenden Anschreiben nach dem Umzug auch eine Vielzahl von Personen erfaßt wird, die ihrer Meldepflicht noch nachkommen würden. Der Vorschlag hätte auch zu einer Portoersparnis geführt.

Um eine Kontrolle über den tatsächlichen Erfolg der Datenübermittlung und ggf. eine Revision der Verordnung zu ermöglichen, sollte eine nachvollziehbare *jährliche Berichtspflicht* des SFB über die aufgrund der regelmäßigen Datenübermittlungen erzielten Mehreinnahmen sowie den hierfür erforderlichen Verwaltungsaufwand in die Verordnung aufgenommen werden.

Leider wurden auch diese Vorschläge nicht aufgegriffen und die Verordnung mit nur minimalen Veränderungen in Kraft gesetzt.[81]. Der Sender Freies Berlin wäre allerdings gut beraten, wenn er auch ohne rechtliche Verpflichtung jährlich die Öffentlichkeit darüber unterrichten würde, wieweit der mögliche Ertrag an zusätzlich eingenommenen Rundfunkgebühren den Verwaltungsaufwand übersteigt.

Rechnung getragen werden sollte, waren für die Senatsverwaltung für Inneres insbesondere folgende Überlegungen von Bedeutung:

Rundfunkanstalten haben ein Interesse an der rechtlichen Gewährleistung der funktionsgerechten Finanzierung des öffentlich-rechtlichen Rundfunks im dualen System und einer gleichmäßigen Gebührenerhebung innerhalb der Rundfunkteilnehmer. Der Rundfunkrat des SFB hat in diesem Zusammenhang darauf hingewiesen, daß nach gesicherten Erkenntnissen 99 % aller Haushalte mindestens ein Hörfunkgerät und 96 % aller Haushalte mindestens ein Fernsehgerät zum Empfang bereithalten. Unter Berücksichtigung der bei der GEZ registrierten Haushalte seien demnach in rund 20 % aller Berliner Haushalte zum Empfang bereitgehaltene Rundfunkgeräte nicht angemeldet. Da die Grundversorgung der Bevölkerung mit Rundfunk Aufgabe der öffentlich-rechtlichen Rundfunkanstalten ist, ist es notwendig, dafür auch die technischen, organisatorischen, personellen und finanziellen Vorbedingungen sicherzustellen. Die Rundfunkanstalten haben einen verfassungsrechtlichen Anspruch darauf, daß ihre Finanzierung gewährleistet ist. Dazu müssen ihnen effiziente Befugnisse an die Hand gegeben werden. Die Rundfunkanstalten sind jedoch nicht nur im eigenen Interesse, sondern auch im Interesse der gerechten Verteilung der Gesamtkosten aller Rundfunkteilnehmer gehalten, alles zu tun, um Teilnehmer ordnungsgemäß zu erfassen.

Nach Auffassung der Senatsverwaltung für Inneres ist eine regelmäßige Datenübermittlung aus dem Melderegister an den SFB bzw. an die GEZ auch im Hinblick auf das informationelle Selbstbestimmungsrecht nicht unverhältnismäßig. Ein Großteil der übermittelten Daten betrifft Personen, die gebührenpflichtig sind und auf deren Daten die Landesrundfunkanstalten einen Rechtsanspruch haben. Dieser Personenkreis kann durch die Datenübermittlung daher nicht beeinträchtigt sein. Der Personenkreis, auf dessen Daten die Landesrundfunkanstalten keinen Anspruch haben, und der damit in seinem informationellen Selbstbestimmungsrecht betroffen ist, ist demgegenüber verschwindend gering. Auch sind die übermittelten Daten nicht von besonderer Sensibilität. Zu berücksichtigen ist ferner, daß nach dem bisherigen Verfahren in einer Vielzahl von Fällen aufgrund veralteter Daten Gebühren entweder zu Unrecht nicht eingezogen oder zu Unrecht eingezogen werden. Die Einnahmeausfälle durch Schwarzhörer und Schwarzseher führen dazu, daß die gesetzestreuen Rundfunkteilnehmer höher belastet werden. Werden Gebühren zu Unrecht eingezogen, so liegt die Meldedatenübermittlung, die diesen Sachverhalt aufdeckt, im Interesse der Betroffenen. Berücksichtigt man im Rahmen der Güterabwägung weiter, daß die übermittelten Daten einer strengen Zweckbindung unterliegen und zur Aufgabenerfüllung nicht mehr benötigte Daten unverzüglich gelöscht werden, dann ist die mit einer regelmäßigen Datenübermittlung von der Meldebehörde an den SFB bzw. an die GEZ verbundene Weitergabe der Daten einer zahlenmäßig sehr kleinen Gruppe, auf die die GEZ keinen Rechtsanspruch hat, verhältnismäßig und zumutbar.

Die Auffassung des Berliner Datenschutzbeauftragten, daß mit der Zulassung der Datenübermittlungen an den SFB bzw. die GEZ eine weitere Durchbrechung des Verwendungszweckes von Meldedaten verbunden sein soll, ist nicht nachvollziehbar. Aufgabe der Meldebehörde ist es u.a. auch, die für die rechtmäßige Erfüllung der Aufgaben öffentlicher Stellen, wozu auch der SFB als öffentlich-rechtliche Rundfunkanstalt gehört, erforderlichen Grunddaten feststellen und nachweisen zu können (§ 1 Abs. 1 Buchstabe a MeldeG). § 26 MeldeG sieht darüber hinaus die grundsätzliche Zulässigkeit von regelmäßigen Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen

vor.

Auch die vom Berliner Datenschutzbeauftragten geäußerte Befürchtung, daß regelmäßige Datenübermittlungen an den SFB bzw. an die GEZ Begehrlichkeiten anderer Stellen wecken könnten, vermag nicht zu überzeugen. Die Situation der von ihm beispielhaft angeführten Versorgungsunternehmen ist mit der Situation der öffentlich-rechtlichen Rundfunkanstalt SFB nicht vergleichbar. Bei der Rundfunkgebühr handelt es sich nicht um eine Gebühr im engeren Sinne, sondern um eine Gebühr mit Beitragselementen. Entscheidend ist nicht die tatsächliche Nutzung, sondern allein die Möglichkeit der Nutzung. Schon diese Möglichkeit löst nach § 4 Abs. 1 des Rundfunkgebührenstaatsvertrages die Gebührenpflicht aus. Eine öffentlich-rechtliche Rundfunkanstalt hat nicht ohne weiteres Möglichkeiten zu kontrollieren, wer die Kriterien, die zur Zahlungspflicht führen, erfüllt. Die Energieversorgungsunternehmen gewähren ihre Leistung erst nach entsprechender Beantragung durch den bzw. nach Vertragsschluß mit dem Nutzer. Im Zweifel können die Energieversorgungsunternehmen ihre Leistungen einfach einstellen.

Auch die Kritik des Berliner Datenschutzbeauftragten, daß von der Meldebehörde mehr Daten übermittelt werden, als die Rundfunkanstalten und die GEZ nach § 3 Abs. 2 des Rundfunkgebührenstaatsvertrages bei den Betroffenen selbst erheben dürfen, vermag nicht zu überzeugen. Eine landesrechtliche Regelung der Zulässigkeit von regelmäßigen Meldedatenübermittlungen an die Landesrundfunkanstalten bzw. an die GEZ wird durch das Rundfunkrecht nicht ausgeschlossen. Zwar enthält der Rundfunkgebührenstaatsvertrag ebenfalls Regelungen zur Ermittlung der Rundfunkteilnehmer bzw. der sie betreffenden Daten; im Rundfunkgebührenstaatsvertrag ist jedoch ausdrücklich klargestellt, daß melderechtliche Regelungen des Landesrechts, die eine Übermittlung von Daten an Landesrundfunkanstalten oder die GEZ zulassen, unberührt bleiben (§ 4 Abs. 6 Satz 2 Rundfunkgebührenstaatsvertrag). Diese Regelung macht deutlich, daß nach den dem Rundfunkgebührenstaatsvertrag zugrunde liegenden Vorstellungen eine systematische bzw. regelmäßige Nutzung der Meldedaten möglich sein soll.

Gegen die vom Berliner Datenschutzbeauftragten angeführte Möglichkeit, in den Meldestellen GEZ-Formulare auszulegen, sind grundsätzlich keine Einwände zu erheben. Eine solche Maßnahme kann jedoch mit Blick auf die beabsichtigten Zwecke nicht als wirksame Alternative zu dem nunmehr ermöglichten Verfahren angesehen werden.

Der Vorschlag des Berliner Datenschutzbeauftragten, die Daten aus dem Melderegister zeitverzögert erst nach drei Monaten zu übermitteln, wurde von der Senatsverwaltung für Inneres nicht aufgegriffen. Personen, die bislang einer bestehenden Rundfunkgebührenpflicht nicht nachgekommen sind, werden in der Regel auch einen Umzug nicht zum Anlaß nehmen, sich bei der GEZ anzumelden. Außerdem liegt auch bereits bei dem durch die erlassene Verordnung geregelten Verfahren ein deutlicher Zeitverzug zwischen Umzug und „Mailing“ durch die GEZ vor, da die Datenübermittlung durch die Meldebehörde nur einmal monatlich erfolgt, so daß bis zum Eingang bei der GEZ bereits bis zu einem Monat ab der melderechtlichen Anmeldung vergeht und auch bei der GEZ nicht jede einzelne Datei sofort verarbeitet wird, sondern die Verarbeitung nur dreimal monatlich erfolgt. Außerdem würde eine Datenübermittlung erst nach drei Monaten die Aktualität des Datenbestandes der Rundfunkteilnehmer beeinträchtigen.

Auch der Vorschlag des Berliner Datenschutzbeauftragten, in die Verordnung eine jährliche Berichtspflicht des SFB über die

aufgrund der regelmäßigen Datenübermittlungen erzielten Mehreinnahmen sowie den hierfür erforderlichen Verwaltungsaufwand aufzunehmen, erschien der Senatsverwaltung für Inneres nicht zweckmäßig zu sein. Es dürfte allenfalls in den ersten Jahren nach Inkrafttreten der Verordnung von Interesse sein, Angaben über erzielte Mehreinnahmen zu erhalten.

Der Senat wird jedoch erwägen, den SFB nach Ablauf eines angemessenen Zeitraums zu bitten, darüber zu berichten, welche Mehreinnahme seit Inkrafttreten der Übermittlungsverordnung erzielt wurden. Einer Festschreibung einer jährlichen Berichtspflicht im Verordnungstext bedarf es dazu nicht.

Keine Melderegisterauskunft bei einer Sperre ?

Eine Bürgerin, für die eine Auskunftssperre nach § 28 Abs. 5 MeldeG im Melderegister gespeichert ist, wurde von der Meldebehörde formularmäßig um Mitteilung gebeten, ob trotz der Sperre aufgrund einer Melderegisteranfrage eine Auskunft erteilt werden darf. Sofern die Petentin nicht einverstanden ist, sollte sie unter Fristsetzung eine detaillierte schriftliche Begründung abgeben. Sollte sie sich innerhalb der Frist nicht äußern, würde von ihrem Einverständnis mit der Bekanntgabe ihrer Anschrift ausgegangen. Dem hatte die Petentin innerhalb der Frist widersprochen. Da der Widerspruch jedoch erst nach Ablauf der Frist einging, wurde die Auskunft erteilt.

Das Landeseinwohneramt fragt bei *Auskunftsersuchen von Privatpersonen oder Firmen* bei dem Betroffenen, der eine Auskunftssperre veranlaßt hat, *immer* schriftlich nach, ob eine Auskunft erteilt werden darf, weil das erfahrungsgemäß bei den meisten Fällen zur Vermeidung von möglichen Nachteilen (beispielsweise bei versäumten Fristen oder bei vergessenen Verbindlichkeiten) ausdrücklich gewünscht werde. Soweit der Betroffene erklärt, daß er eine Auskunftserteilung nicht wünscht, wird das Auskunftsersuchen ohne weitere Wertung abschlägig beschieden. Bei Verdacht eines Mißbrauches werden die Betroffenen bei einer Ablehnung der Auskunftserteilung aufgefordert, dies detailliert zu begründen. Wenn der Betroffene nicht widerspricht und keine Anhaltspunkte dafür vorliegen, daß aus der Erteilung der Melderegisterauskunft eine Gefährdung erwachsen könnte, wird eine Auskunft erteilt. Die Anhörung des Betroffenen wird auf § 14 MeldeG gestützt, wonach der Meldepflichtige auf Verlangen der Meldebehörde die Auskünfte zu geben hat, die für die ordnungsgemäße Führung des Melderegisters benötigt werden. Wenn der Betroffene sich nicht meldet, wird hieraus geschlossen, daß er konkludent in die Auskunftserteilung einwilligt.

Nach § 28 Abs. 5 MeldeG ist *jede* Melderegisterauskunft unzulässig, wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, daß ihm oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlich schutzwürdige Belange erwachsen kann. Soweit dem Antrag auf Auskunftssperre stattgegeben worden ist, sind keine Auskünfte aus dem Melderegister an Privatpersonen oder andere nichtöffentliche Stellen mehr zulässig.

Wir haben das Verfahren, trotz Auskunftssperre an bestimmte Unternehmen Auskünfte zu erteilen, bereits im Jahr 1989 bemängelt[82]. Nach den Beratungen im Unterausschuß Datenschutz des Abgeordnetenhauses hatte die Senatsverwaltung für Inneres das Landeseinwohneramt angewiesen, künftig diese Praxis ein-

Es ist zutreffend, daß die Senatsverwaltung für Inneres im Jahre 1990 das Landeseinwohneramt Berlin angewiesen hatte, bei Vorliegen einer Auskunftssperre das bis dahin praktizierte Verwaltungsverfahren bezüglich der Erteilung von Auskünften aus dem Melderegister zu ändern.

Bis zu diesem Zeitpunkt erteilte das Landeseinwohneramt Berlin einigen bestimmten Institutionen (wie z.B. Banken, Kreditinstituten usw.) grundsätzlich auch dann eine Melderegisterauskunft, wenn im Datensatz der betroffenen Person eine Auskunftssperre eingetragen war. Dabei ging das Landeseinwohneramt davon aus, daß bei Auskünften an diese Institutionen eine Gefährdung für den Betroffenen nicht eintritt und somit entsprechende Auskünfte erteilt werden können. Ferner wurden Auskünfte trotz einer eingetragenen Auskunftssperre erteilt, wenn das Interesse des Antragstellers an der Erteilung der Auskunft das Interesse des Betroffenen an der Verweigerung der Auskunft überwog.

Die seinerzeitigen Beanstandungen des Berliner Datenschutzbeauftragten bezüglich dieses Verfahrens sowie das Ergebnis der Beratungen im Unterausschuß „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin hatte die Senatsverwaltung für Inneres dann zum Anlaß genommen, das Landeseinwohneramt Berlin mit Blick auf den Wortlaut des § 28 Abs. 5 MeldeG sowie den insoweit gleichlautenden Wortlaut des § 21 Abs. 5 MRRG anzuweisen, künftig eingetragene Auskunftssperren gegenüber jedermann gelten zu lassen. Dies hatte zur Folge, daß auch für eine im Einzelfall vorzunehmende Güterabwägung kein Raum mehr war. Damit wurde dem Petitum des Berliner Datenschutzbeauftragten entsprochen.

Das Landeseinwohneramt Berlin hat in der Folgezeit bei Anfragen zu Personen, bei denen eine Sperre im Meldedatensatz eingetragen war, diese Personen über die vorliegende Anfrage unterrichtet und um Mitteilung gebeten, ob jeweils im konkreten Fall trotz eingetragener Sperre eine Auskunft erteilt werden

[82] vgl. JB 1989, 4.4

zustellen. Das geschilderte Verfahren steht hierzu im Widerspruch. Eine Auskunftserteilung ist bei Bestehen einer Auskunftssperre nur dann zulässig, wenn der Betroffene zuvor seine ausdrückliche Einwilligung erteilt hat. Sofern er sich im Anhörungsverfahren nicht äußert oder nicht förmlich in die Auskunftserteilung einwilligt, ist diese nach § 28 Abs. 5 MeldeG unzulässig. Zwar muß das Landeseinwohneramt als Meldebehörde bei dem Verdacht eines Mißbrauches der Auskunftssperre prüfen, ob diese zu widerrufen ist; dies hat jedoch – sofern die Voraussetzungen dafür vorliegen – in einem gesonderten Verfahren *vor* Erteilung einer Melderegisterauskunft zu geschehen. Aus diesem Grund darf auch nicht verlangt werden, daß jede Ablehnung einzelner Auskunftsersuchen gesondert begründet wird.

darf. Dabei zeigte sich in zahlreichen Fällen, daß die betroffenen Personen der Erteilung von Auskünften über ihre Person grundsätzlich nicht zustimmten; auch dann nicht, wenn ihnen aus der Erteilung einer Auskunft ganz offensichtlich keine Gefahr im Sinne des § 28 Abs. 3 MeldeG erwachsen würde. In vielen Fällen entstand auch der begründete Verdacht, daß Personen die ihnen einmal bewilligte Auskunftssperre nunmehr dazu mißbrauchen, um sich dem Zugriff ihrer privaten Gläubiger zu entziehen. Wenn dies im Einzelfall die Durchsetzung bestehender zivilrechtlicher Ansprüche erheblich erschwert, führt dies immer wieder zu einer Verärgerung und zu Unverständnis bei dem jeweiligen Antragsteller.

Das Melderegister ist zwar gemäß den melderechtlichen Regelungen kein öffentliches Register, gleichwohl tragen die Vorschriften über die Erteilung einer Melderegisterauskunft im privaten Bereich dem dort bestehenden Informationsbedürfnis bewußt Rechnung. Die melderechtlichen Vorschriften über die Erteilung einer Melderegisterauskunft gehen grundsätzlich davon aus, daß jedermann erreichbar sein soll und es hinnehmen muß, daß andere Mitbürger notfalls staatliche Hilfe erwarten, um mit ihm Kontakt aufnehmen zu können. Dies hat insbesondere auch dann zu gelten, wenn ein Gläubiger die aktuelle Anschrift seines Schuldners benötigt, um gegen ihn seine zivilrechtlichen Forderungen eintreiben zu können.

Es kann auch nicht Sinn und Zweck einer eingetragenen Auskunftssperre sein, sich mit ihrer Hilfe dem Zugriff der Gläubiger entziehen zu können. Eine Auskunftssperre soll verhindern, daß dem Betroffenen oder einer anderen Person aus der Erteilung einer Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann. Wenn jedoch der begründete Verdacht entsteht, daß der Betroffene die Auskunftssperre dazu mißbraucht, um sich mit ihrer Hilfe dem Zugriff seiner Gläubiger zu entziehen, hat die Meldebehörde erneut zu prüfen, ob die Voraussetzungen für die eingetragene Auskunftssperre noch vorliegen und ggf. in einem gesonderten Verfahren auch über eine Rücknahme der Auskunftssperre zu entscheiden.

Um einen möglichen Mißbrauch beurteilen zu können, ist es jedoch erforderlich, daß der Betroffene zumindest in den Fällen, in denen ein konkretes Auskunftsersuchen allem Anschein nach nicht im Zusammenhang mit der Bedrohungssituation steht, darlegt, warum er in diesem Fall bei der Erteilung einer Melderegisterauskunft gleichwohl eine Gefährdung im Sinne des § 28 Abs. 5 MeldeG für sich oder eine andere Person sieht.

Die Erfahrungen der meldebehördlichen Praxis sind leider häufig die, daß Personen, denen aus bestimmten Gründen eine Auskunftssperre bewilligt wurde, sich damit gänzlich ihrer Umwelt und ihren Verantwortlichkeiten entziehen möchten. Aus diesen Gründen werden die Betroffenen vom Landeseinwohneramt Berlin auch bereits bei Einrichtung einer Auskunftssperre darauf hingewiesen, daß ihnen bei allen Auskunftsersuchen grundsätzlich Gelegenheit zur Äußerung gegeben wird, ob die Bekanntgabe der Wohnanschrift ihrer Auffassung nach eine Gefährdung zur Folge haben könnte. Ihnen wird ferner mitgeteilt, daß sie dann gehalten sind zu antworten, wenn die Wohnanschrift nicht bekanntgegeben werden soll. Sie werden deshalb auch ausdrücklich auf die Möglichkeit hingewiesen, bei vorhersehbarer längerer Abwesenheit (Urlaub, Krankenhaus, Kur usw.) entsprechende Postnachsendeanträge zu stellen oder dem Landeseinwohneramt über die längere Abwesenheitszeit eine Nachricht zukommen zu lassen. Die Begründung einer entsprechenden Verpflichtung zur Äußerung ist gemäß § 14 MeldeG zulässig und auch erforderlich, weil anderenfalls die Betroffenen durch einfaches Schweigen und Untätigbleiben eine sachgerechte Beurteilung eines möglichen Mißbrauchs der für

sie eingetragenen Auskunftssperre verhindern könnten. Den Betroffenen wird auch schon bei der Bewilligung ihrer Auskunftssperren hinreichend verdeutlicht, daß ihre Einwilligung unterstellt und eine Auskunft erteilt wird, wenn sie nicht antworten. Der Auffassung des Berliner Datenschutzbeauftragten, daß eine Auskunftserteilung nach § 28 Abs. 5 MeldeG unzulässig ist, wenn ein Betroffener sich im Anhörungsverfahren nicht äußert, vermag der Senat nicht zuzustimmen. Anhörung des Betroffenen bedeutet in diesem Zusammenhang lediglich, daß ihm Gelegenheit zur Äußerung gegeben werden muß (siehe hierzu auch Kommentar von Belz zum Meldegesetz für Baden-Württemberg, RN 20 zu § 33). Dabei ist dem Betroffenen für seine Äußerung eine angemessene Frist zu setzen und ihm gleichzeitig mitzuteilen, daß die Meldebehörde davon ausgeht, daß aus seiner Sicht gegen die beantragte Auskunft keine Bedenken bestehen, wenn innerhalb der Frist keine gegenteilige Äußerung eingeht.

Das Landeseinwohneramt setzt dem Betroffenen dabei eine Äußerungsfrist von vier Wochen. Diese Frist ist nach Auffassung des Senats auch ausreichend. (Nach der o.a. Kommentierung von Belz zum Meldegesetz für Baden-Württemberg sollte die Frist im Regelfall nicht weniger als zwei Wochen betragen, wobei diese Frist sich allerdings noch verkürzen könne, wenn der Antragsteller ein dringendes Bedürfnis für eine alsbaldige Auskunftserteilung glaubhaft mache.)

Auch in dem vom Berliner Datenschutzbeauftragten angeführten Einzelfall ist das Landeseinwohneramt Berlin so verfahren. Da eine Äußerung der Betroffenen innerhalb der Monatsfrist nicht vorlag, mußte das Landeseinwohneramt von dem Einverständnis der Betroffenen für eine Auskunftserteilung ausgehen. Das Landeseinwohneramt hat dementsprechend eine Auskunft erteilt, wobei sogar zum Zeitpunkt der Auskunftserteilung noch elf weitere Tage seit Ablauf der gesetzten einmonatigen Frist vergangen waren. Erst nachdem dann eine Auskunft erteilt worden war, ging beim Landeseinwohneramt ein Schreiben der Betroffenen ein, mit dem sie mitteilte, daß sie mit einer Auskunftserteilung nicht einverstanden sei. Festzustellen bleibt im übrigen noch, daß der Betroffenen aus der Auskunftserteilung keine Gefährdung im Sinne des § 28 Abs. 5 MeldeG entstanden ist.

Der Senat vermag nicht zu erkennen, daß das vom Landeseinwohneramt Berlin praktizierte Verfahren gegen § 28 Abs. 5 MeldeG verstößt. Der Senat erachtet vielmehr das hier praktizierte Verfahren als durchaus sachgerecht.

Der Untermieter und das leidige Problem mit der Steuerkarte

Pünktlich mit der Verteilung der Lohnsteuerkarten für das neue Jahr erreichen uns alljährlich wieder die Beschwerden von Betroffenen, die zur Untermiete wohnen, weil in ihrer Steuerkarte der Hauptmieter als Adressierungszusatz aufgeführt ist.

Die bei der Anmeldung erhobenen Daten des Wohnungsgebers dürfen nach § 2 Abs. 2 Nr. 6 MeldeG nur für den dort genannten Zweck – nämlich die *Feststellung der Mitwirkungspflichtigen* nach § 13 MeldeG – erhoben und gespeichert werden[83]. Die weitergehende Verwendung des Namens des Wohnungsgebers als Adressierungszusatz ist dagegen nicht durch § 2 Abs. 1 Nr. 11 MeldeG abgedeckt, da danach lediglich gegenwärtige und frühere Anschriften sowie die Haupt- und Nebenwohnung gespeichert werden dürfen, nicht aber, in welchem privatrechtlichen Verhältnis der Betroffene

Die Auffassung des Berliner Datenschutzbeauftragten, daß der Name des Wohnungsgebers nicht als Adressierungszusatz verwendet werden dürfe, wird vom Senat nicht geteilt. Dies ergibt sich schon daraus, daß in Blatt 1212 des Datensatzes für das Meldewesen (Einheitlicher Bundes-/Länderteil) – DSMeld – bei dem Datum „Anschrift“ der Wohnungsgeber eine eigene Feldbezeichnung hat. Nach der Beschreibung des Feldinhaltes ist der Wohnungsgeber anzugeben, soweit dies zur Adressierung erforderlich ist. Da der Inhalt des DSMeld in den Fällen, in denen in Rechtsvorschriften (z.B. 1. und 2. BMeldDÜV) auf ihn

[83] JB 1988, 4.5

zum Wohnungsgeber steht und welchen Namen der Wohnungsgeber hat. Die Senatsverwaltung für Inneres war seinerzeit lediglich bereit, in den Erläuterungen zu den Feldern des Meldescheines die Erhebung selbst näher zu erklären, ohne aber von der bisherigen Praxis des Speicherns des Adressierungszusatzes Abstand zu nehmen.

Das hat zur Folge, daß bei den Altfällen nicht nur bei Melderegisterauskünften nach den §§ 28, 29 MeldeG an Private oder Datenübermittlungen an andere öffentliche Stellen nach den §§ 25 bis 27 MeldeG, sondern auch bei den Lohnsteuerkarten, die aufgrund des Datenbestandes des Melderegisters erstellt werden, diese Adressierungszusätze „bei“ nach der eindeutigen Zweckbestimmung des § 2 Abs. 2 Nr. 6 MeldeG unzulässigerweise ausgedruckt werden und bei Melderegisterauskünften oder für Arbeitgeber Rückschlüsse auf die persönlichen und sachlichen Verhältnisse des Betroffenen möglich sind. Für eine Löschung des Namens des Wohnungsgebers als Adressierungszusatz bedarf es allerdings eines Antrages des Bürgers, der erst danach eine neue Lohnsteuerkarte ausgestellt bekommt.

Hier ist durch technisch-organisatorische Maßnahmen sicherzustellen, daß bei den Altfällen der Adressierungszusatz sowohl bei den Melderegisterauskünften oder den Übermittlungen an andere öffentliche Stellen als auch bei der Erstellung der Lohnsteuerkarten beim Ausdruck weggelassen wird.

Bezug genommen wird, rechtlich verbindlich ist, kann die Angabe des Wohnungsgebers bei der Anschrift von Untermietern grundsätzlich nicht beanstandet werden.

Das Landeseinwohneramt Berlin löscht allerdings im Meldedatensatz die Angabe des Wohnungsgebers als Adressierungszusatz bei dem Datum „Anschrift“, wenn der Betroffene dieses wünscht. Der Senat hält diese Verfahrensweise für ausreichend. Er hält es dagegen nicht für angezeigt, den Adressierungszusatz in den vom Berliner Datenschutzbeauftragten angesprochenen Altfällen bei den Melderegisterauskünften oder den Übermittlungen an andere öffentliche Stellen oder auch bei der Erstellung der Lohnsteuerkarten wegzulassen. Insbesondere im Zusammenhang mit der Ausstellung der Lohnsteuerkarten würde das Weglassen des Adressierungszusatzes auch in zahlreichen Fällen zu Beschwerden der Betroffenen darüber führen, daß die Lohnsteuerkarten deshalb nicht ordnungsgemäß zugestellt werden konnten.

Eine Befragung der Personen, die von diesen sogenannten Altfällen betroffen sind (es handelt sich hierbei um ca. 100 000 Datensätze), ob sie mit einer weiteren Speicherung und Nutzung des von ihnen bei ihrer Anmeldung angegebenen Adressierungszusatzes weiterhin einverstanden sind, ist wegen der Kosten für den Schriftverkehr und des Verwaltungsaufwandes für die Bearbeitung dieses Schriftverkehrs nicht vertretbar.

Nach sechs Jahren Zuzugsort noch immer Ostberlin’

Bei Anmeldungen von Bewohnern aus dem Ostteil der Stadt wurde bis zur Wende im Melderegister als früherer Wohnort Ostberlin’ gespeichert. Ein Betroffener, der von der Speicherung im Rahmen einer Selbstauskunft Kenntnis erlangt hat, empfand diesen Zusatz als nicht mehr zeitgemäß.

Im Melderegister dürfen Anschriften nur dann gespeichert werden, wenn es sich um Wohnungen handelt, die sich zum Zeitpunkt der Anmeldung im Geltungsbereich des Melderechtsrahmengesetzes (MRRG) befanden (§ 2 Abs. 1 Nr. 11 und Abs. 2 Nr. 7 MeldeG). Wohnungen außerhalb des Bereiches, in dem die Rechtsordnung der Bundesrepublik gilt, haben für die melderechtliche Behandlung außer Betracht zu bleiben (§ 17 Abs. 1 MeldeG). Die Anschriften von Wohnungen in der ehemaligen DDR oder auch nur der allgemeine Hinweis Ostberlin’ dürfen nur mit Einwilligung des Betroffenen oder bis zum 16. Lebensjahr mit der Einwilligung des Personensorgeberechtigten gespeichert werden (§ 11 Abs. 3 Satz 2 MeldeG). Das Problem im Einzelfall wurde durch die Löschung der Daten gelöst. Wir gehen davon aus, daß auch in anderen Fällen so verfahren wird. Dessenungeachtet sollte bei Gelegenheit eine Löschung von Amts wegen erfolgen.

Die zuständige Senatsverwaltung wird die Angelegenheit überprüfen und ggf. einer Lösung zuführen.

4.2.2 Personenstandswesen

Die Bundesregierung hat zwei Gesetzentwürfe zur Änderung des Personenstandsgesetzes vorgelegt. Mit dem Entwurf eines *Gesetzes zur Neuordnung des Eheschließungsrechtes*[84] wird empfohlen, das *Aufgebot abzuschaffen*, dessen öffentlicher Aushang nicht erforderlich ist. Dies entspricht einer langjährigen Forderung der Datenschutzbeauftragten. Der noch nicht im Bundestag eingebrachte Entwurf eines Fünften Gesetzes zur *Änderung des Personenstandsgesetzes* (PStÄndG) berücksichtigt weitgehend die seit Jahren vorgetragenen Forderungen der Datenschutzbeauftragten des Bundes und der Länder, die in Personenstandsbücher einzutragenden Angaben auf die Daten zu beschränken, die für

Der Berliner Datenschutzbeauftragte wird im Rahmen der üblichen Bund-Länder-Erörterungen über den aktuellen Sachstand zum Vorentwurf eines Fünften Gesetzes zur Änderung des Personenstandsgsetzes in Kenntnis gesetzt werden.

[84] BT-Drs. 13/4898

den Beurkundungszweck selbst von Bedeutung sind.

Mit der an das Bundesarchiv angelehnten Regelung soll es für die Nutzung der Personenstandsbücher künftig genügen, ein berechtigtes Interesse darzulegen, wenn seit dem Tod des Betroffenen mindestens 30 oder – falls der Todestag nicht bekannt ist – seit der Geburt mindestens 120 Jahre vergangen sind. Damit dürfte eine datenschutzgerechte Regelung gefunden sein, die in Zukunft insbesondere die *Ahnenforschung* in angemessener Weise erleichtert.

Weiterhin wird mit der an das Melderecht angelehnten Regelung des § 61 Abs. 5 PStÄndG der besonderen Gefährdungssituation einzelner Betroffener Rechnung getragen. Nach dem Glaubhaftmachen der Gefährdung wird bei den Personenstandseinträgen ein *Sperrvermerk* eingetragen. Dann dürfen ohne Einwilligung des Betroffenen Personenstandsurkunden nur erteilt und Auskünfte und Einsicht nur gewährt werden, wenn es zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im überwiegenden Interesse eines Dritten liegenden Gründen unerläßlich ist.

Trotz dieser erfreulichen Entwicklung halten wir Änderungen noch für erforderlich.

So soll eine Befugnis zur *regelmäßigen Datenübermittlung der Meldebehörde* geschaffen werden. Ungeachtet der verfassungsrechtlichen Frage, ob der Bundesgesetzgeber befugt ist, über Art. 75 Grundgesetz hinaus im Personenstandsgesetz unmittelbar verbindliches Melderecht zu schaffen, ist die vorgesehene Regelung im Hinblick auf § 18 Abs. 4 Melderechtsrahmengesetz und § 26 Abs. 1 MeldeG unzureichend. Regelmäßige Datenübermittlungen dürfen danach nur erfolgen, soweit dies durch Bundes- oder Landesrecht unter Feststellung des Anlasses und des Zweckes der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. Der Entwurf bestimmt zwar den Anlaß sowie den Datenempfänger, nicht jedoch den Zweck und vor allem nicht die zu übermittelnden Daten. Die Pflicht der Meldebehörde zur Datenübermittlung an das Standesamt sollte besser in den Landesmeldegesetzen und in den dazu erlassenen Meldedatenübermittlungsverordnungen (in Berlin: DVO-MeldeG) geregelt werden.

Dem Entwurf ist auch nicht zu entnehmen, welche weiteren Stellen welche Daten an das Standesamt übermitteln müssen. Die übermittelnden Stellen werden kaum in der Lage sein zu entscheiden, welche Daten der Standesbeamte für die Eintragung in das Personenstandsbuch benötigt. Darüber hinaus gehören die vorgesehenen Übermittlungen der Gerichte in ein Justizmitteilungsgesetz.

Bei der *Nutzung zu Forschungszwecken* sollte in Anlehnung an § 30 BlnDSG festgelegt werden, daß die Übermittlung der vorherigen Zustimmung der obersten Landesbehörde oder einer ihr bestimmten Stelle bedarf und diese den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen sowie das Forschungsvorhaben bezeichnen muß und dem Landesdatenschutzbeauftragten mitzuteilen ist.

Auffällig ist die Diskrepanz zwischen der Erhebungsbefugnis der Behörden (Personen-standsdaten dürfen von Behörden lediglich zur Erfüllung hoheitlicher Aufgaben verlangt werden) und der *Übermittlungsbefugnis des Standesamtes* (die Übermittlung von Personenstandsdaten an Behörden und sonstige öffentliche Stellen durch die Standesbeamten ist zulässig, wenn diese zur Erfüllung der in der Zuständigkeit des Empfängers liegenden – also auch nicht-hoheitlichen – Aufgaben erforderlich ist).

Aus dem Gesetzentwurf selbst läßt sich nicht ersehen, daß die Übermittlung nach Maßgabe einer Rechtsverordnung erfolgen soll und daß es sich hier um Mitteilungs*pflichten* des Standesamtes handelt. Dies ergibt sich lediglich aus der Begründung. Wenn es schon dem Verordnungsgeber überlassen bleiben soll, Behörden zu bestimmen, denen der Standesbeamte Personenstandsdaten zu übermitteln hat, so erfordern es die vom Bundesverfassungsgericht im Volkszählungsurteil entwickelten Kriterien, daß wegen des mit den Übermittlungen verbundenen Eingriffes in das Recht auf informationelle Selbstbestimmung eine normenklare gesetzliche Regelung zu schaffen ist, die spezifische Aussagen über Voraussetzung, Umfang und Empfänger der Datenübermittlungen enthält. Der Entwurf erfüllt diese Voraussetzungen nicht.

4.2.3 Ausländerangelegenheiten

Großzügige Fahndung nach Ausländern

Aufgrund einer Ausschreibung im INPOL-Fahndungsbestand, die der Polizeipräsident für die Ausländerbehörde vorgenommen hatte, wurde ein ehemaliger jugoslawischer Staatsbürger in einem anderen Bundesland von der Polizei festgenommen. Als Grund für die Speicherung im Fahndungsbestand wurde „Festnahme zur Ausweisung/Abschiebung" angegeben. Am folgenden Tag erfuhr die Polizei, die den Betroffenen festgenommen hatte, von der Berliner Ausländerbehörde, daß eine Abschiebung derzeit nicht möglich sei, eine Löschung der Daten im Fahndungsbestand jedoch nicht erfolge, da eine Abschiebung in naher Zukunft erfolgen könne. Der Betroffene wurde daraufhin nach 14 Stunden im Polizeigewahrsam entlassen.

Ungeachtet der Frage, warum die Klärung hier nicht schneller erfolgen konnte, ist dieser Umgang der Ausländerbehörde mit dem polizeilichen Fahndungsbestand nicht akzeptabel.

Nach den *INPOL-Grundsätzen* trägt der Polizeipräsident als die Stelle, die die Daten in den Fahndungsbestand eingibt, die Verantwortung für die Richtigkeit und Aktualität der Daten. Das ist durch eine Prüfungsverpflichtung der Ausländerbehörde, die die Speicherung veranlaßt, sicherzustellen.

Angesichts des erheblichen Eingriffes, der mit der Ausschreibung zur Fahndung verbunden ist, und der Verantwortlichkeit der Polizeibeamten, die sich bei der Festnahme einer Person auf die Aktualität des Datenbestandes verlassen müssen, ist nicht hinnehmbar, daß eine Datenspeicherung im Fahndungsbestand verbleibt, wenn Abschiebungshindernisse bekanntwerden.

Die Prüfung, ob die Abschiebung nunmehr möglich oder ob einem Ausländer die Duldung oder eine längere Ausreisezeit zuzubilligen ist, rechtfertigt eine Festnahme – und damit eine Fahndungsausschreibung – nicht. Eine Rechtsgrundlage hierfür ist nicht ersichtlich.

Werden bei einem Ausländer, den die Ausländerbehörde zur Festnahme ausgeschrieben hat, Abschiebungshindernisse bekannt oder wird der Betroffene vorübergehend oder endgültig von der Ausreisepflicht befreit, ist die Löschung der Ausschreibung bei der für Eingabe zuständigen Polizeidienststelle unverzüglich zu veranlassen.

Entgegen den Ausführungen des Berliner Datenschutzbeauftragten ist der Umgang der Berliner Ausländerbehörde mit dem polizeilichen Fahndungsbestand weder bezüglich der Ausschreibung zur Festnahme noch hinsichtlich der Löschung dieser Daten zu beanstanden.

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

- ausgewiesen worden und nach Ablauf der Ausreisefrist untergetaucht ist,
- als abgelehnter Asylbewerber nach Ablauf der Ausreisefrist untergetaucht ist und in beiden Fällen, die Abschiebung auch möglich ist

oder

- ein Ausländer abgeschoben wurde.

Sie hat den Zweck,

a) die Abschiebung in den Heimatstaat oder einen dritten Staat zu ermöglichen,
b) behördlich auf den Straftatbestand des illegalen Aufenthalts reagieren zu können und
c) das bestehende Einreise- und Aufenthaltsverbot auch nach Verlassen des Bundesgebiets durchsetzen zu können.

Die Behörde, die die Ausschreibung veranlaßt hat, hat ihr bekannt gewordene Veränderungen der Voraussetzungen für die Ausschreibung zu berücksichtigen und die notwendigen Veränderungen zu veranlassen. Dies geschieht auch bei der Berliner Ausländerbehörde und – soweit bekannt ist – bundesweit anlaß- und einzelfallbezogen. Insofern geht die Kritik ins Leere.

Der Zweck der Ausschreibung zur Festnahme entfällt allerdings nicht in jedem Einzelfall schon dann, wenn die Abschiebung in den Heimatstaat vorübergehend nicht mehr erreicht

werden kann, weil dieser Staat seine Bürger ohne ein Rückführungsabkommen nicht aufnimmt. So war es im vom Berliner Datenschutzbeauftragten dargestellten Fall.

Für die Berliner Ausländerbehörde bestand erst Grund, die Löschung der Ausschreibung durch den Polizeipräsidenten in Berlin zu veranlassen, als die Möglichkeit der Abschiebung in ein Drittland von der jeweils zuständigen Ausländerbehörde geklärt worden war. Das war im vorliegenden Falle die für den Ort der Festnahme zuständige Behörde des anderen Bundeslandes gewesen. Die Polizei hat diese Behörde jedoch nicht angesprochen. Das wäre jedoch auch im Interesse des Ausländers erforderlich gewesen. Dies ist bedauerlich, kann aber nicht der Praxis der Berliner Ausländerbehörde angelastet werden.

Wenn nicht abgeschoben worden wäre, hätte er eine Duldung oder eine längere Ausreisefrist erhalten, was ihm die Sicherung vor weiteren Festnahmen gebracht hätte. In diesem Zusammenhang hätte die zuständige Ausländerbehörde auch die Löschung der Ausschreibung über die Berliner Ausländerbehörde im INPOL veranlaßt.

Angemerkt sei noch, daß die im Bericht des Datenschutzbeauftragten aufgestellte Behauptung, die Berliner Ausländerbehörde habe sich mit der Aussage, eine Löschung der Daten im Fahndungsbestand erfolge nicht, da eine Abschiebung in nächster Zeit erfolgen könne, auf der Auskunft eines Polizeibeamten beruht. Dieser will dies telefonisch von einer Sachbearbeiterin der Ausländerbehörde erfahren haben. Ob diese Äußerung tatsächlich so gefallen ist, war nicht mehr nachzuvollziehen. Es sei noch einmal betont, daß sie sich jedenfalls nicht mehr mit der oben dargestellten behördlichen Praxis deckt.

Datenverarbeitung beim Rückübernahmeabkommen mit Vietnam

Die Bundesregierung hat mit der Regierung von Vietnam ein Rückübernahmeabkommen abgeschlossen. Diese machte die Bearbeitung davon abhängig, daß die Rückkehrwilligen eine Reihe von teils recht persönlichen Fragen beantworteten. Hierzu legte das Landeseinwohneramt allen vietnamesischen Staatsbürgern einen Fragebogen sowie ein Erläuterungsschreiben vor.

Das Ausfüllen des gesamten Fragebogens ist freiwillig. Die Erhebung der Daten des Betroffenen kann danach nur auf dessen Einwilligung (§ 10 Abs. 1 i.V.m. § 6 Abs. 1 Nr. 3 BlnDSG) gestützt werden. Diese ist vom Betroffenen schriftlich einzuholen. Zuvor ist er umfassend *über die Bedeutung der Einwilligung aufzuklären.*

Das bei der Ausländerbehörde praktizierte Verfahren entsprach nicht den genannten Grundsätzen. Das Formschreiben, das die Betroffenen zur Erläuterung erhielten, bezeichnete lediglich die Beantwortung bestimmter Fragen als freiwillig und erweckte im übrigen den Eindruck, es bestehe die Verpflichtung, den Fragebogen „Selbstangabe" auszufüllen. Es enthielt zudem den irreführenden Hinweis „Gemäß § 70 des Ausländergesetzes (...) sind Sie zur Mitwirkung in dieser Angelegenheit verpflichtet." Mitwirkungen nach dieser Bestimmung betreffen nicht die Freiwilligkeit, das – auf Wunsch der vietnamesischen Seite in das Verfahren aufgenommene – Formular auszufüllen, sondern gelten für das Verfahren an sich. Darüber hinaus enthält der Fragebogen zahlreiche Fragen, die für die Durchführung der Rückführung nach Vietnam und die hierfür notwendige Identifikation der Betroffenen nicht erforderlich sind. Wir haben die Praxis der Datenerhebung beanstandet und empfohlen klarzustellen, daß

Die Darstellung des Berliner Datenschutzbeauftragten

- das Ausfüllen des gesamten in Rede stehenden Fragebogens sei freiwillig,
- die Daten können nur auf die Einwilligung des Betroffenen gestützt werden,
- die Einwilligung sei schriftlich einzuholen, und
- zuvor sei eine Aufklärung des Betroffenen vorzunehmen,

ist rechtlich unzutreffend. Aus diesem Grunde wurde die Forderung des Berliner Datenschutzbeauftragten auch nicht aufgegriffen.

Rechtsgrundlage für die Aufforderung, den Fragebogen auszufüllen, ist § 6 Abs. 1 Nr. 2 des Berliner Datenschutzgesetzes und nicht §§ 6 Abs. 1 Nr. 3 Abs. 3-5 und 10 dieses Gesetzes. Die erhobene Daten sind für die Durchsetzung der Ausreisepflicht nach § 42 Abs. 1 Ausländergesetz erforderlich, da die Republik Vietnam generell auf der vollständigen Übermittlung dieser Daten besteht. Die Rechtmäßigkeit der Datenerhebung ergibt sich aus § 75 Abs. 1 Ausländergesetz. Danach dürfen die mit der Ausführung dieses Gesetzes betrauten Behörden zum Zwecke der Ausführung dieses Gesetzes personenbezogenen Daten erheben, soweit dies zur Erfüllung ihrer Aufgaben

[85] vgl. BVerfG – 2 BvR 96/95

die Entscheidung, das Formular nicht oder nicht vollständig auszufüllen, nicht zu Nachteilen führt.

Unserer Anregung, das Aufklärungsschreiben den Betroffenen auch *in vietnamesischer Sprache* vorzulegen, begegnete das Landeseinwohneramt mit dem Hinweis, eine derartige Verpflichtung sei nicht erkennbar. Die Amtssprache sei deutsch, und entsprechende Haushaltsmittel seien nicht verfügbar. Daß Aufklärungsrechte von Betroffenen nicht nach Maßgabe vorhandener Haushaltsmittel zur freien Disposition gestellt werden können, erklärt sich von selbst. Zu den Anforderungen, die an eine wirksame Aufklärung von Ausländern in einem fairen Verwaltungsverfahren zu stellen sind, hat das Bundesverfassungsgericht im vergangenen Jahr festgestellt[85]:

„Es ist zu berücksichtigen, daß der Asylbewerber sich in einer ihm fremden Umgebung befindet, mit dem Ablauf des deutschen Asylverfahrens nicht vertraut und in aller Regel der deutschen Sprache nicht mächtig ist. (...) Es ist demnach erforderlich, daß dem Asylbewerber durch eine erläuternde Belehrung mit der gebotenen Deutlichkeit vor Augen geführt wird, welche Obliegenheiten ihn im einzelnen treffen und welche Folgen bei deren Nichtbeachtung entstehen können. (...). Diesem Gebot wird in aller Regel schon durch die in der ganz überwiegenden Anzahl der Fälle erforderliche Übersetzung der Vorschriften in *eine dem Asylbewerber geläufige Sprache* genügt, weil sich dabei aus Gründen der Praktikabilität eine sinngemäße, *nicht strikt an juristischen Begrifflichkeiten orientierte Übertragung anbietet.*"

Seltsamerweise wurde uns im nachhinein mitgeteilt, daß das Formular doch in vietnamesischer Sprache vorlag.

In Art. 1 Nr. 2 Satz 4 des Protokolls zur Durchführung des Abkommens über die Rücknahme vietnamesischer Staatsangehöriger ist bestimmt, daß der *Antrag auf Ausstellung eines Paßersatzes* ausgefüllt werden soll, wenn der Fragebogen nicht oder nicht vollständig beantwortet wird. Kann der Betroffene gültige Reisedokumente vorlegen, ist diese Datenerhebung nicht erforderlich und damit unzulässig. Dennoch wurde jedem Formschreiben – aus Gründen der Verwaltungsökonomie – ein *Antrag auf Ausstellung eines Paßersatzes* als Anlage beigefügt.

Als Reaktion auf unsere Beanstandung hat die Senatsverwaltung für Inneres das Landeseinwohneramt gebeten, die Betroffenen ausdrücklich – in einem Formschreiben, das auch in vietnamesischer Sprache bereitgestellt wird – auf die Freiwilligkeit der Angaben hinzuweisen. Ferner wurde uns mitgeteilt, daß künftig auf das Ausfüllen eines Paßantragsformulars verzichtet werde, wenn der Betroffene über gültige Reisedokumente verfügt. Unseren weitergehenden Empfehlungen, die Betroffenen ausführlich über die Bedeutung der Einwilligung – insbesondere über den Verwendungszweck der Daten und die beabsichtigte Übermittlung nach Vietnam – aufzuklären, wurde nicht nachgekommen.

ASYL-CARD

Eine Arbeitsgruppe zur Harmonisierung der Verwaltungsabläufe zwischen Bund und Ländern im Asylverfahren hat vorgeschlagen, eine Asyl-CARD einzuführen. Als Beispiel dient die in den Niederlanden bereits für alle Bürger eingeführte „Smart-Card". Sie wird dort zur Zeit als Identitätsnachweis, zu Meldezwecken und als Berechtigungsnachweis für den Bezug von Leistungen verwendet. Zur Vorbereitung wird erwogen, eine „Machbarkeitsstudie" in Auftrag zu geben.

nach diesem Gesetz erforderlich ist.

Dem Berliner Datenschutzbeauftragten ist dagegen beizupflichten, daß „Aufklärungsrechte von Betroffenen nicht nach Maßgabe vorhandener Haushaltsmittel zur freien Disposition" der Verwaltung stehen. Dies wurde aber – auch durch die Berliner Ausländerbehörde – zu keiner Zeit behauptet. Durch die Ausländerbehörde wurde lediglich darauf verwiesen, daß hier keine Aufklärungsrechte vollziehbar ausreisepflichtiger Ausländer bestehen, und daß aus diesem Grunde auch eine Rechtspflicht zur Übersetzung des Formschreibens nicht existiere, da die Amtssprache deutsch sei. Diesen Hinweis auf geltendes Recht, der sich auch mit der zitierten Entscheidung des Bundesverfassungsgerichts deckt, vermögen wir nicht zu beanstanden.

Im übrigen wurde dem Berliner Datenschutzbeauftragten zu keinem Zeitpunkt mitgeteilt, daß das Formschreiben ausschließlich in deutscher Sprache versandt wurde. Aus Gründen einer bürgernahen Verwaltung wurden und werden die ausreisepflichtigen vietnamesischen Staatsangehörigen in vietnamesischer Sprache angeschrieben.

Zutreffend sind dagegen die Ausführungen, wonach bis zur Beanstandung des Berliner Datenschutzbeauftragten das Bezeichnen der Angaben zu Fragen des Fragebogens als freiwillig und dem Verweis auf § 70 Ausländergesetz der Eindruck vermittelt wurde, die sonstigen Angaben dieses Fragebogens seien auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet. Das Landeseinwohneramt Berlin wurde daher gebeten, ausdrücklich auf die Freiwilligkeit der Angaben nach § 6 Abs. 2 BlnDSG i.V.m. § 13 Abs. 3 BDSG hinzuweisen. Auch die Beanstandung, daß das Ausfüllen eines Paßantragsformulars auch dann erfolgte, wenn der Betroffene über gültige Reisedokumente verfügte, trifft zu. Das Landeseinwohneramt Berlin wurde auch hier gebeten, von seiner Verfahrenspraxis abzurücken. Beides ist auch geschehen. Die Versäumnisse werden bedauert.

Dieses Projekt wirft die Frage auf, unter welchen Voraussetzungen multifunktionale Identitätskarten akzeptabel sind. Beschränken sich Chipkarten auf einzelne, klar definierte Funktionen wie etwa die Krankenversichertenkarte, gibt es keine grundsätzlichen Einwände gegen dieses Medium. Werden jedoch mehrere Bereiche eingezogen wie hier melderechtliche, ausländerrechtliche und sozialrechtliche, bergen diese Karten das Risiko, daß die bestehenden Verwertungsbeschränkungen wie etwa das Sozialgeheimnis nicht mehr gewahrt werden. Zudem besteht die Gefahr, daß der Umfang der Daten, die auf derartigen Karten gespeichert werden, ständig wächst.

Da die Machbarkeitsstudie noch nicht vorliegt, können nähere Aussagen noch nicht gemacht werden. Es fragt sich aber grundsätzlich, warum die neue multifunktionale Chipkartentechnologie gerade an einer Bevölkerungsgruppe wie den Asylbewerbern ausprobiert werden soll, bei denen wahrlich andere Probleme als der Einsatz von Hightech zu lösen sind[86].

Die Ausführungen sind zwischenzeitlich überholt. Das Bundesministerium des Innern plant nunmehr, die Erstellung einer Machbarkeitsstudie auszuschreiben. Eine Leistungsbeschreibung für diese Studie wurde den Innenministerien und -senatsverwaltungen der Länder übermittelt.

Die Senatsverwaltung für Inneres hat diese am 3. März 1997 unmittelbar nach Erhalt an den Berliner Datenschutzbeauftragten weitergeleitet.

Eine Stellungnahme des Berliner Datenschutzbeauftragten steht hierzu noch aus.

4.2.4 Straßenverkehr

Obwohl die Umsetzung der EU-Richtlinie des Rates v. 29. Juli 1991 über den Führerschein (91/439/EWG),[87] spätestens zum 1. Juli 1996 hätte erfolgen müssen, hat die Bundesregierung den Entwurf eines Gesetzes zur Änderung des *Straßenverkehrsgesetzes* und anderer Gesetze (StVG–E) erst jetzt in den Bundestag eingebracht[88].

Ziel der Gesetzesänderung ist auch die Überarbeitung der fahrerlaubnisrechtlichen Regelungen in datenschutzrechtlicher Hinsicht. Diesem Anspruch wird der Entwurf nur teilweise gerecht. Die Datenerhebungsbefugnisse der Fahrerlaubnisbehörde sind in dem Entwurf beispielsweise nur unzureichend geregelt. Der Entwurf trifft zwar eine Regelung darüber, welche Daten die Fahrerlaubnisbehörde zur Prüfung, ob der Antragsteller zum Führen eines Kraftfahrzeuges geeignet und befähigt ist, erheben darf; in der Gesetzesbegründung heißt es dagegen, daß die Regelung der *Datenerhebungsbefugnisse* nicht abschließend sei. Dem Gebot der Normenklarheit wird eine nicht abschließende Regelung der Datenerhebungsbefugnisse jedoch nicht gerecht. Der Antragsteller kann dem Gesetzestext nicht entnehmen, bei welchen Stellen die zuständige Fahrerlaubnisbehörde Daten über seine Person erheben darf.

Der Gesetzentwurf enthält – im Gegensatz zu einem Vorentwurf[89] – auch Regelungen über die *Vernichtung von Unterlagen*. Für Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse sieht er eine Vernichtung spätestens nach zehn Jahren vor, es sei denn, die Unterlagen stehen im Zusammenhang mit einer Eintragung im Verkehrszentralregister oder im Zentralen Fahrerlaubnisregister (§ 2 Abs. 9 StVG–E). Wir werden uns dafür einsetzen, daß die Zehn-Jahres-Frist durch eine differenzierte landesrechtliche Regelung ausgefüllt wird. Die Zehn-Jahres-Frist ist nach Vorstellung des Gesetzgebers die oberste zeitliche Grenze, nach der spätestens Unterlagen zu vernichten/Daten zu löschen sind. Die in dem Gesetzentwurf eingeräumte Möglichkeit, anstelle einer Vernichtung der Daten eine Sperrung vorzunehmen, verstehen wir als absolute Ausnahmeregelung. Bedauerlich ist die Regelung, daß Unterlagen in „Altakten" nur dann vernichtet werden müssen, wenn die Fahrerlaubnisbehörde aus einem anderen Anlaß mit der Akte befaßt ist. Erst 15 Jahre nach Inkrafttreten des Gesetzes sollen alle Akten „bereinigt" sein.

Der Gesetzentwurf, der im Februar 1997 dem Bundestag zugeleitet worden ist, enthält eine Vielzahl von bereichsspezifischen Regelungen über die Erhebung, Nutzung und Löschung von Daten. Diese Regelungen hat das federführende Bundesministerium für Verkehr mit dem Datenschutzreferat des Bundesministeriums der Justiz und dem Bundesbeauftragten für den Datenschutz abgestimmt.

Der Senat hält den Gesetzentwurf für ausgewogen; die aufgenommenen Datenschutzregelungen stellen einen vernünftigen Kompromiß zwischen dem Interesse der Öffentlichkeit an der Sicherheit des Straßenverkehrs und dem informationellen Selbstbestimmungsrecht des Einzelnen dar. Die Normen entsprechen rechtsstaatlichen Anforderungen, denn sie sind hinreichend bestimmt. Auslegungsbedürftigkeit macht nach ständiger Rechtsprechung des Bundesverfassungsgerichts eine Norm nicht unbestimmt.

86 vgl. hierzu sehr treffend die Glosse im Spiegel Nr.5/1997, S. 17
87 Amtsblatt der EG Nr. L237 v. 24. August 1991
88 BR-Drs. 821/96; vgl. JB 1995, 5.12
89 JB 1995, 5.12

Prüfung der Führerscheinstelle

Im Berichtszeitraum wurde die Führerscheinstelle beim Landeseinwohneramt daraufhin überprüft, inwieweit die eigene Arbeitsanweisung über die Verwaltung, Aufbewahrung und Aussonderung der Akten des Referates III C umgesetzt wird und welche Unterlagen die Vorgänge bei der Ersterteilung, Neuerteilung und Versendung an den Gutachter enthalten.

Die Straßenverkehrsvorschriften enthalten bisher keine Regelungen über die Dauer der *Aufbewahrung der Unterlagen* in den Akten. Somit ist auf die allgemeinen Bestimmungen des ASOG zurückzugreifen. Nach § 42 Abs. 1 ASOG können die Ordnungsbehörden rechtmäßig erhobene personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit das zur Erfüllung ihrer Aufgaben erforderlich ist. Das Speichern personenbezogener Daten ist nur dann erforderlich, wenn die gesetzlich zugewiesene Aufgabe sonst nicht oder nicht vollständig erfüllt werden könnte. Es genügt nicht, daß die Speicherung die Aufgabenerfüllung erleichtert. Der Grundsatz der Erforderlichkeit beschränkt die Speicherung auch in zeitlicher Hinsicht. Erforderlich ist die Speicherung erst dann, nur solange und in dem Umfang, wie die Aufgabe in Bezug auf den Betroffenen aktuell ist. Ein Vorhalten von Daten zum Zweck der Gefahrenabwehr hat zu unterbleiben, wenn die Belange des Betroffenen im Hinblick auf die – geringfügige – Wahrscheinlichkeit und Schwere der drohenden Gefahr unverhältnismäßig beeinträchtigt werden. Soweit die Aufgabenerfüllung die Speicherung nicht (mehr) erfordert, muß sie unterbleiben, noch gespeicherte Daten sind zu löschen.

Bei der Beurteilung der Erforderlichkeit der Speicherung können schon jetzt die dargestellten Regelungen des StVG–E herangezogen werden. Die Löschungsfrist für Führungszeugnisse und Registerauszüge gilt auch für die den Eintragungen zugrundeliegenden Entscheidungen. Würden z.B. Urteile oder Entscheidungen wegen einer Ordnungswidrigkeit über die Löschungsfrist im Verkehrszentralregister hinaus aufbewahrt werden, würde dies dem Resozialisierungsgedanken der Löschungsregelungen widersprechen. Künftig soll nach Ablauf der Tilgungsfrist ein umfassendes gesetzliches *Verwertungsverbot* gelten (§ 29 Abs. 8 StVG–E). Die bisher unbefristete Verwertungsmöglichkeit nach § 52 Bundeszentralregistergesetz (BZRG) wird abgeschafft. Damit dürfen die Tat und die Entscheidung dem Betroffenen nach der Tilgung im Verkehrszentralregister nicht mehr vorgehalten werden. Das setzt eine Vernichtung der Unterlagen voraus, die sich auf die getilgten und im Register gelöschten Entscheidungen beziehen. Die Senatsverwaltung für Bauen, Wohnen und Verkehr hat mitgeteilt, über Vorab-Regelungen nachdenken zu wollen, sobald sich abzeichnet, in welcher Form das StVG in Kraft treten wird.

Wegen eines Korruptionsfalles und des Wunsches der Polizei, die Unterlagen bis zum Schluß der Ermittlungen vorrätig zu halten, waren bei der Prüfung die nach der Geschäftsanweisung über die Aufbewahrung der Unterlagen nach drei Jahren zu vernichtenden *Erstanträge* von 1992 noch komplett vorhanden. Diese Unterlagen sind für die ordnungsgemäße Aufgabenerfüllung der Führerscheinstelle nicht mehr erforderlich, sie werden ausschließlich für Ermittlungszwecke der Polizei weiter aufbewahrt. Somit sind die Daten zu sperren (§ 48 Abs. 6 ASOG). Sie dürfen nur noch zu den in § 48 Abs. 6 Satz 1 ASOG genannten Zwecken genutzt werden. Das bedeutet, daß schon die Kenntnisnahme – und nicht nur die Verwendung – gesperrter Daten außerhalb der gesetzlich geregelten Ausnahmefälle ausgeschlossen und gewährleistet sein muß, daß der *Zugang zu den gesperrten Datenbeständen* nur bei Vorliegen der gesetzlichen Voraussetzungen eröffnet wird (Zugangssicherung,

Die an dieser Stelle geäußerte Auffassung des Berliner Datenschutzbeauftragten über die Führung und Aussonderung von Akten und die Aussonderung von Aktenteilen steht im Widerspruch zur höchstrichterlichen Rechtsprechung. Das Bundesverwaltungsgericht hat sich in einer Entscheidung vom 16. März 1988 mit dieser Frage befaßt und unter anderem folgendes festgestellt:

> „Die Pflicht zur Aktenführung soll den Geschehensablauf wahrheitsgetreu und vollständig dokumentieren und dient damit in zweifacher Weise der Sicherung gesetzmäßigen Verwaltungshandelns. Die Dokumentation soll den Geschehensablauf so, wie er sich ereignet hat, in jeder Hinsicht nachprüfbar festhalten. Sie soll hierbei nicht lediglich den Interessen der Betroffenen oder der entscheidenden Behörde dienen, sondern auch die Grundlage für die kontinuierliche Wahrnehmung der Rechts- und Fachaufsicht und für die parlamentarische Kontrolle des Verwaltungshandelns bilden. Damit wirkt die Pflicht zur wahrheitsgetreuen und vollständigen Aktenführung zugleich auch präventiv insofern auf das Verwaltungshandeln ein, als sie die Motivation zu allseits rechtmäßigem Verwaltungshandeln stärkt und rechtswidriges Verwaltungshandeln erschwert. Diese Sicherung gesetzmäßigen Verwaltungshandelns durch wahrheitsgetreue und vollständige Aktenführung dient auch dem Schutz derjenigen Betroffenen, deren persönliche Daten in den Akten festgehalten sind und über die die Akten gegebenenfalls Nachteiliges oder Belastendes enthalten; auch sie werden durch die wahrheitsgetreue und vollständige Dokumentation des Geschehensablaufs in der dargelegten Weise vor nicht rechtmäßigem Verwaltungshandeln geschützt.
>
> Die Pflicht zur Führung wahrheitsgetreuer und vollständiger Akten kann ihre präventive und ihre nachträgliche Sicherungsfunktion nur entfalten, wenn die Akten so lange aufbewahrt werden, daß sie ihre Nachweisfunktion im Bedarfsfall tatsächlich erfüllen können. Es kann deshalb keine Rede davon sein, daß sie zur Vermeidung von Verletzungen des Rechts auf informationelle Selbstbestimmung schon dann vernichtet werden müßten, wenn kein Betroffener mehr aktuelle Ansprüche gegen die Behörde erheben und diese die Akten nicht mehr zur Grundlage von aktuellen Maßnahmen gegen einen Betroffenen oder zugunsten eines Betroffenen machen könnte.
>
> ...
>
> Eine Vernichtung von Akten kann deshalb nur für einen Zeitpunkt in Betracht gezogen werden, in dem mit Sicherheit feststeht, daß die Akten ihre die Gesetzmäßigkeit der Verwaltung sichernde Dokumentationsfunktion nicht mehr erfüllen.“ (Neue Zeitschrift für Verwaltungsrecht 1988 S. 621, 622)

Das Bundesverwaltungsgericht hat in seiner Entscheidung allerdings die Frage offen gelassen, wie die Fristen für die Vernichtung von Akten oder Aktenteilen zu bemessen sind.

Die noch geltenden straßenverkehrsrechtlichen Vorschriften enthalten keine Regelungen über die Daten der Aufbewahrung

Zugangskontrolle). Derzeit haben alle Beschäftigten der Führerscheinbehörde einen unkontrollierten Zugang zu den Unterlagen und die Möglichkeit, die gesperrten Daten zur Kenntnis zu nehmen.

In den Ordnern mit sog. „Listenvorgängen" sind Unterlagen mit unterschiedlich langen Aufbewahrungsfristen abgelegt. Wegen der unterschiedlichen Fristen werden Unterlagen zu lange aufbewahrt, weil die Vorgänge einerseits jahrgangsweise geführt und auch so vernichtet, andererseits jedoch nicht zwischenzeitlich gesondert auf zu vernichtendes Schriftgut durchgesehen werden. Die Aktenführung ist so zu organisieren, daß eine fristgemäße Vernichtung der Unterlagen erfolgt.

Die Führerscheinstelle hat wiederholt selbst *Führungszeugnisse* über Antragsteller eingeholt. Nach § 31 BZRG ist dies nur zulässig, soweit es zur Erledigung von hoheitlichen Aufgaben benötigt wird *und* eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist oder erfolglos bleibt. Der Betroffene kann bei der Beantragung des Führungszeugnisses bei der Meldestelle verlangen, daß es – wenn es Eintragungen enthält – zunächst an ein von ihm bestimmtes Amtsgericht zur Einsichtnahme durch ihn übersandt wird (§ 30 Abs. 5 BZRG). Auf diese Möglichkeit ist er durch die Meldestelle bei der Antragstellung hinzuweisen. Nach der Einsichtnahme wird das Führungszeugnis an die Behörde weitergeleitet oder – falls der Antragsteller widerspricht – vom Amtsgericht vernichtet. In den von uns überprüften Akten waren – bis auf eine Ausnahme – keine Gründe dokumentiert, warum eine Aufforderung an den Betroffenen, das Führungszeugnis selbst anzufordern, unterblieben ist.

Die Akten enthielten *Anklageschriften* und *Urteile* von Strafgerichten. Eine Entscheidung befaßte sich nur mit dem unentschuldigten Fernbleiben des Angeklagten in der Hauptverhandlung. Eine andere Akte enthielt die Anklageschrift zu einem anhängigen Verfahren wegen der Verletzung der Unterhaltspflicht. Weiterhin haben wir mehrere Strafurteile wegen Diebstahls vorgefunden. Bei einem Urteil wegen Körperverletzung bestand auch nach Einschätzung des LEA in einem Vermerk kein straßenverkehrsrechtlicher Bezug. Weiterhin haben wir Urteile wegen Vergehen gegen das Fernmeldegesetz oder die Ausfertigung eines Haftbefehles vorgefunden. Ein anderer Vorgang enthielt ein Urteil vom 9. April 1985 (Jugendstrafe wegen Diebstahl).

Es ist nicht feststellbar, für welchen Zweck diese Unterlagen zu den Vorgängen genommen wurden und aufbewahrt werden. Ein straßenverkehrsrechtlicher Bezug ist regelmäßig ebensowenig erkennbar wie fahrerlaubnisrechtliche Folgen. Sie sind für die ordnungsgemäße Aufgabenerfüllung nicht bzw. bei einer über zehn Jahre zurückliegenden Straftat als Jugendlicher nicht mehr erforderlich. Diese Einschätzung wird ausweislich von Vermerken hinsichtlich der Verwertung geteilt. Darüber hinaus sind die in den Urteilen oder Anklageschriften aufgeführten Daten Dritter (Zeugen, Mittäter) nicht erforderlich. Eine Speicherung ist demzufolge nicht von § 42 Abs. 1 ASOG gedeckt.

Nach den §§ 12, 15 b und 15 c der Straßenverkehrszulassungsordnung (StVZO) kann die Verwaltungsbehörde unter den in diesen Vorschriften näher bezeichneten Voraussetzungen u.a. anordnen, daß der Inhaber oder Bewerber einer Fahrerlaubnis das Gutachten einer amtlich anerkannten *medizinisch-psychologischen Untersuchungsstelle* oder eines amtlich anerkannten

von Unterlagen in Führerscheinakten. Das neue Straßenverkehrsgesetz, das im Zuge der Umsetzung der 2. EU-Führerscheinrichtlinie gegen Mitte 1998 in Kraft treten soll, enthält jedoch bereichsspezifische Regelungen über die Erhebung und Speicherung von Daten und über Aussonderungsfristen für zu den Akten genommene Registerauskünfte, Führungszeugnisse und Kraftfahreignungsgutachten. Nach dem Gesetzentwurf der Bundesregierung, der im Februar 1997 dem Bundestag zugeleitet worden ist, müssen die genannten Unterlagen im Zuge der laufenden Bearbeitung nach spätestens 10 Jahren aus den Führerscheinakten entfernt werden. Sogenannte Altakten müssen nach einer Übergangsbestimmung des Gesetzes nach spätestens 15 Jahren bereinigt werden.

Der Senat begrüßt diese Regelungen, da sie zweifelsfrei festlegen, welche Unterlagen wann entfernt werden müssen und insoweit Rechtsklarheit schaffen.

Die vom Berliner Datenschutzbeauftragten zitierte Vorschrift des § 31 BZRG über die Einholung von Führungszeugnissen ist der Führerscheinstelle des Landeseinwohneramtes bekannt. Führungszeugnisse werden von Amts wegen nur dann eingeholt, wenn eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist. Dies ist in der Regel dann der Fall, wenn die Führerscheinstelle die Entziehung der Fahrerlaubnis vorbereitet. Es ist davon auszugehen, daß kein Betroffener – schon wegen der damit verbundenen Kosten – ein Führungszeugnis vorlegen würde, wenn er erfährt, daß die Behörde dieses benötigt, um Verwaltungsmaßnahmen gegen ihn zu treffen. Die Auffassung des Berliner Datenschutzbeauftragten, in jedem Fall seien in der Führerscheinakte die Gründe zu dokumentieren, warum ein Führungszeugnis nach der Vorschrift des § 31 BZRG von Amts wegen angefordert worden ist, teilt der Senat nicht.

Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr über die körperliche und geistige Eignung zum Führen von Kraftfahrzeugen beizubringen hat.

Nach den Eignungsrichtlinien teilt die Verwaltungsbehörde den Betroffenen unter Darlegung der Gründe für die Zweifel an seiner Eignung und unter Angabe der für die Begutachtung in Betracht kommenden Stellen mit, daß er sich innerhalb einer Frist auf seine Kosten der Begutachtung zu unterziehen hat. Zugleich fordert sie den Betroffenen auf, die Zustimmung zur Übersendung der für die Begutachtung *erforderlichen* Verwaltungsvorgänge an den Gutachter zu erteilen. Diese Beschränkung hat zur Folge, daß nur die Teile des Vorganges an den Gutachter übersandt werden dürfen, die im Hinblick auf die Eignungsfragen Aufschluß über den Betroffenen geben können. Demgegenüber wurde in allen geprüften Fällen die komplette Akte an den Gutachter übersandt. Zuvor wurden Retente angelegt, die Kopien der Anordnung zur Beibringung des Gutachtens, der Zustimmungserklärung, des Auftrages an den Gutachter, des Bildes und einer vorbereiteten neuen Karteikarte sowie der Anfrage an die Polizei enthalten. Dabei handelt es sich offensichtlich um die Unterlagen, die die Führerscheinstelle für ihre Arbeit für erforderlich hält. Eine Durchsicht der Führerscheinakte daraufhin, ob sie Unterlagen enthält, die für die Begutachtung nicht erforderlich sind, um diese dann den Retenten zuzuordnen, erfolgt nicht.

Auf keinen Fall sind für den Gutachter folgende von uns vorgefundene Unterlagen erforderlich: Kassenbelege, Lesedurchschriften, Postzustellungsurkunden, Anträge auf Ersatzführerscheine, eingezogene und entwertete Führerscheine, telefonische Vorausmeldungen über die Beschlagnahme, Mitteilungen über das Ende der Sperrzeit, Belege über gezahlte Verwaltungsgebühren, Fahrerlaubnisanträge, Aktenanforderungen, Anforderungen von Karteikartenabschriften, Mitteilungen an das Kraftfahrtbundesamt, Schriftwechsel mit den Antragstellern über Terminvereinbarungen, Melderegisteranfragen und -auskünfte, Meldungen der Post über den Fund eines Führerscheines, Mitteilungen an den Betroffenen über den Punktestand, Ausfertigung eines Haftbefehles.

Verschiedentlich wurden formularmäßig sog. *Überwachungsaufträge* an die Polizei erteilt. Es wurde um Überprüfung gebeten, ob Betroffene trotz des Fahrerlaubnisentzuges ein Kfz führen. Die Polizei erstellte ihrerseits einen Bericht, der dann zur Akte genommen wird. Die Überwachungsaufträge sollen die Mitteilung eines Anfangsverdachtes des Vorliegens einer Straftat (§ 21 StVG) im Rahmen von § 44 ASOG sein. Künftig sind diese Übermittlungen nach § 3 Abs. 5 StVG–E auch geregelt. Nach der Begründung zum Gesetz soll die Polizei die Entscheidung der Fahrerlaubnisbehörde auf deren Einhaltung hin überwachen können.

Gegen die Mitteilung eines Verdachtes des Vorliegens einer Straftat nach § 21 StVG bestehen keine Bedenken; Voraussetzung ist allerdings, daß den Betroffenen die erforderliche Fahrerlaubnis zum Führen eines Kraftfahrzeuges fehlt und ein konkreter, begründeter Verdacht vorhanden ist. Nur die Tatsache, daß er weiter Halter eines Kraftfahrzeuges ist, genügt dazu regelmäßig nicht, weil das Kraftfahrzeug ein Angehöriger fahren oder aber dies versicherungstechnische Gründe haben kann. Die Übermittlung des Ergebnisses und die Speicherung des Berichtes der Polizei in der Akte ist allerdings nicht erforderlich (§ 9 Abs. 1 BlnDSG). Sofern der Betroffene tatsächlich ein Fahrzeug geführt hat, ist ein Strafverfahren einzuleiten. Im Fall einer Verurteilung erhält die Führerscheinstelle das Ergebnis im Rahmen der Anordnung über Mitteilungen in Straftaten (MiStra) übermittelt. Hat der Betroffene allerdings kein

Fahrzeug geführt, besteht keine Notwendigkeit zur Speicherung der Tatsache, wann er sich wo aufgehalten hat. Das entspricht auch den Intentionen des StVG–E, wonach diese Übermittlungen der Überwachung des Straßenverkehrs im Allgemeinen und nicht der Überwachung des Einzelnen dienen sollen.

Die Benachrichtigungen des Kraftfahrtbundesamtes über einen Punktestand von neun und mehr Punkten aufgrund von Eintragungen in das Verkehrszentralregister werden dauernd in den Akten aufbewahrt. Die Tilgungsfrist im Verkehrszentralregister beträgt zwei Jahre bei Entscheidungen über eine Ordnungswidrigkeit (§ 13 a Abs. 2 Nr. 1 Straßenverkehrszulassungsordnung (StVZO)) und fünf Jahre (§ 13 a Abs. 2 Nr. 2 StVZO), wenn auf Geldstrafe erkannt worden ist. Nach Ablauf der Tilgungsfrist der letzten Verkehrszentralregistereintragung ist eine Aufbewahrung der Benachrichtigungen über den Punktestand nicht mehr erforderlich und widerspricht dem Resozialisierungsgedanken der Löschungsfristen im Verkehrszentralregister.

Die Akten sind um die nicht erforderlichen Unterlagen *anlaßbezogen zu bereinigen*. In den Unterlagen (z.B. Urteilen), die für die Aufgabenerfüllung noch erforderlich sind, sind die Daten Dritter anlaßbezogen datenschutzgerecht zu schwärzen.

Zur Frage, ob Unterlagen aus den Führerscheinakten entfernt werden müssen, bevor diese einer medizinisch-psychologischen Untersuchungsstelle übersandt werden, hat die für den Verkehrsbereich zuständige Senatsverwaltung dem Berliner Datenschutzbeauftragten mit Schreiben vom 29. April 1994 mitgeteilt, daß der aus den Eignungsrichtlinien zitierte Passus („die für die Begutachtung erforderlichen Verwaltungsvorgänge“) nicht so zu verstehen sei, daß die Behörde ihre Akten nach eigenem Gutdünken in einen „wichtigen“ und einen „unwichtigen“ Teil aufspalten muß. Diese Auffassung teilt der Senat. In der Tatsache, daß die Führerscheinstelle des Landeseinwohneramtes Berlin unter Hinweis auf dieses Schreiben eine weitere Erörterung der Angelegenheit ablehnt, sieht der Senat insofern keinen Verstoß gegen die Verpflichtung zur Unterstützung des Berliner Datenschutzbeauftragten.

Leider will das Landeseinwohneramt in den wesentlichen Punkten unseren Empfehlungen nicht folgen, es lehnt vielmehr hinsichtlich der Aktenübersendung an den Gutachter eine weitere Erörterung ab. Das stellt nicht nur einen Verstoß gegen die Unterstützungspflicht (§ 28 BlnDSG) dar, sondern ist insofern auch bemerkenswert, weil dies der Auslöser für die Prüfung war. Im übrigen existieren in anderen Bundesländern Regelungen zur Bereinigung von Akten, so u.a. wann Urteile und Strafbefehle zu entfernen sind.

Regelmäßige Anfrage bei der Polizei

Im Zusammenhang mit der Erteilung oder Verlängerung der Geltungsdauer der Fahrerlaubnis zur Fahrgastbeförderung fragt die Führerscheinstelle regelmäßig bei der Polizei an, ob dort abgeschlossene oder laufende Ermittlungsverfahren gespeichert sind.

Anfragen bei der Polizei dürfen nur erfolgen, soweit hierfür im Einzelfall Anlaß besteht. Sie haben sich auf laufende Verfahren zu beschränken[90]. Regelmäßige Anfragen bei der Polizei und die regelmäßige Übersendung kompletter ISVB-Auszüge haben zu unterbleiben, wie dies auch der Praxis in anderen Bundesländern entspricht. In seiner Stellungnahme zu unserem Jahresbericht 1995 hat der Senat unsere Auffassung geteilt[91]. Darüber hinaus unterliegen personenbezogene Daten, die die Polizei im Rahmen von strafrechtlichen Ermittlungsverfahren gewonnen hat und zur vorbeugenden Straftatenbekämpfung weiterspeichert, einer Zweckbegrenzung.

Es trifft nicht zu, daß der Senat in seiner Stellungnahme zum Jahresbericht die Auffassung des Berliner Datenschutzbeauftragten, nach der Regelanfragen beim ISVB zu unterbleiben haben, geteilt hat. Dem Berliner Datenschutzbeauftragten ist bekannt, daß der Senat eine solche Regelanfrage in Verfahren, die die Erteilung oder der Verlängerung der Geltungsdauer einer Fahrerlaubnis zur Fahrgastbeförderung (Omnibusführerschein, Taxischein) dienen, im Interesse der zu befördernden Fahrgäste für notwendig hält. Dies ist dem Berliner Datenschutzbeauftragten – zuletzt mit

[90] JB 1995, 5.12
[91] Drs. 13/595

Bericht des Berliner Datenschutzbeauftragten	Stellungnahme des Senats

Sie dürfen nur zum Zweck der vorbeugenden Straftatenbekämpfung genutzt werden (§ 42 Abs. 3 ASOG). Datenübermittlungen der Polizei an die Fahrerlaubnisbehörde, die über laufende Verfahren hinausgehen, sind deshalb unzulässig. Dem entspricht im übrigen das vom LEA verwandte Formular, mit dem ausdrücklich nach *anhängigen* Verfahren gefragt wird.

Der Polizeipräsident lehnt eine Änderung des Verfahrens ab.

Schreiben vom 12. Februar 1996 – mitgeteilt worden.

Der Senat weist darauf hin, daß die Polizei nach § 44 Abs. 1 ASOG befugt ist, personenbezogene Daten zur Erfüllung ordnungsbehördlicher Aufgaben den Ordnungsbehörden zu übermitteln. Wenn diese Übermittlung auf Ersuchen der Ordnungsbehörde, z. B. der Führerscheinstelle geschieht, hat die Polizei nach § 44 Abs. 5 ASOG nicht die Zulässigkeit der Übermittlung zu prüfen.

§ 42 Abs. 3 ASOG wird vom Datenschutzbeauftragten falsch wiedergegeben. Die Vorschrift enthält nur eine Öffnungsklausel für die Nutzung von Strafverfolgungsdaten für Zwecke der Gefahrenabwehr. Eine wie auch immer geartete Nutzungsbeschränkung enthält § 42 Abs. 3 ASOG nicht.

Identitätskontrollen bei der Fahrerlaubnisprüfung

Dem TÜV Berlin/Brandenburg war bei der Durchführung der Fahrerlaubnisprüfung wiederholt aufgefallen, daß ausländische Bewerber andere Personen zur Ablegung ihrer Prüfung vorgeschickt haben und zu diesem Zweck die Personaldokumente durch Austauschen des Lichtbildes verfälscht worden waren. Der TÜV hatte daraufhin Kopien der Personaldokumente gefertigt und zu den Prüfungsunterlagen genommen, um dem Landeseinwohneramt die Möglichkeit zu geben, die Manipulationen aufzudecken.

Für die hier vorgenommene Speicherung der *Lichtbilder* gab es keine Rechtsgrundlage, die die Speicherung der Daten durch den TÜV erlaubt hätte. Dies ist auch von der Senatsverwaltung für Bauen, Wohnen und Verkehr so gesehen worden. Verwundert hat uns allerdings die Art und Weise, wie die Senatsverwaltung die technischen Prüfstellen über die Unzulässigkeit der Datenerhebung und -speicherung unterrichtet hat. In dem Schreiben an die technischen Prüfstellen heißt es: „Da eine spezielle Rechtsgrundlage für diese Form der Datenerhebung fehlt und der Berliner Datenschutzbeauftragte in solchen Fällen – ungeachtet der Sachargumente – regelmäßig einen formalen Rechtsstandpunkt vertritt, bitten wir darum, dieses Verfahren aufzugeben." Die unzulässig erhobenen Daten sind inzwischen gelöscht.

Das vom Berliner Datenschutzbeauftragten beschriebene Verfahren hat der TÜV Berlin-Brandenburg e.V. ohne Absprache mit der zuständigen Senatsverwaltung für Bauen, Wohnen und Verkehr eingeführt, weil es wiederholt zu Betrugsversuchen bei der theoretischen Fahrerlaubnisprüfung gekommen war. Das Verfahren ist aufgegeben worden, nachdem der Berliner Datenschutzbeauftragte das Fehlen einer Rechtsgrundlage für die sachlich an sich gebotene Datenspeicherung bemängelt hatte.

Parkraumbewirtschaftung in Berlin

Im Jahresbericht 1995[92] hatten wir über das Parkraumbewirtschaftungskonzept berichtet, wonach private Firmen in drei festgelegten Parkraumbewirtschaftungsgebieten in Berlin u.a. mit der Überwachung des ruhenden Verkehrs beauftragt sind. Wir hatten unsere datenschutzrechtlichen Bedenken im Zusammenhang mit dem Parkraumbewirtschaftungskonzept dargestellt.

Inzwischen hat das Amtsgericht Tiergarten[93] den Einsatz Privater zur Überwachung des ruhenden Verkehrs als einen Verstoß gegen die der Polizei übertragene *hoheitliche Aufgabe der Verfolgung von Verkehrsordnungswidrigkeiten* angesehen (§ 26 StVG). Das Kammergericht[94] hat die Entscheidung des Amtsgerichts bestätigt.

Noch vor der Entscheidung des Amtsgerichtes hatten wir eine datenschutzrechtliche Prüfung bei einer der privaten Betreiberfirmen durchgeführt. Dabei sind wir auf zahlreiche datenschutzrechtliche Mängel gestoßen.

92 JB 1995, 3.5
93 304 a OWi 467/96
94 Beschluß 2 Ss 171/96

So hat die Betreiberfirma die Negative der von den Mitarbeitern zu Beweiszwecken gefertigten Fotos offen zugänglich für sämtliche Mitarbeiter der Firma aufbewahrt. Die Negative sind damit nicht gegen den Zugriff Unbefugter gemäß § 5 Abs. 2 BlnDSG geschützt. Die Betreiberfirma hat die bei der Parkraumkontrolle erhobenen und dann gespeicherten Daten nach Abgabe der Bänder an die Bußgeldstelle auf ihrem PC nicht gelöscht, wie dies nach dem Vertrag mit dem Land Berlin ihre Pflicht gewesen wäre. Es fanden sich noch Datenkopien aller bisher erhobenen Daten. Der genutzte Einzelplatzcomputer war nicht durch Sicherheitstools geschützt. Nur die ausgewählte Anwendersoftware verfügte über ein Identifizierungs- und Authentifizierungsverfahren. Es kann nicht gewährleistet werden, daß das Eindringen eines „normalen" Benutzers auf die Betriebssysteme verhindert wird. Eine Eingabeprotokollierung der Dateneingaben hat nach unseren Feststellungen nicht stattgefunden.

Da eine Bundesratsinitiative zur Änderung des Straßenverkehrsgesetzes, durch die eine Übertragung der Überwachung des ruhenden Verkehrs zugelassen werden sollte, kaum Aussicht auf Erfolg hat, ist inzwischen geplant, für die Parkraumbewirtschaftung beim Polizeipräsidenten einen Betrieb des Landes Berlin zu gründen. Ob diese Konstruktion den Ansprüchen an eine hoheitliche Aufgabenerfüllung entspricht, ist zweifelhaft und dürfte dann ebenfalls einer gerichtlichen Klärung zugeführt werden. Jetzt ist vor allem für eine ordnungsgemäße Abwicklung zu sorgen, d.h. sicherzustellen, daß die bei den Firmen vorhandenen Daten restlos gelöscht und – soweit sie für die Aufgabenerfüllung der Polizei erforderlich sind – vollständig übergeben werden.

Der Berliner Datenschutzbeauftragte hat mit Schreiben vom 13. Februar 1997 bestätigt, daß den festgestellten datenschutzrechtlichen Mängeln im wesentlichen abgeholfen ist. Mit Beendigung der Verträge zum 31. März 1997 werden keine personenbezogenen Daten von den Betreiberfirmen der Parkraumbewirtschaftung mehr erhoben. Die privaten Überwacher waren nach dem Amtsgerichtsurteil vom 24. April 1996 noch als Verwaltungshelfer der Polizei eingesetzt. Ab 1. April 1997 wird die Überwachung des ruhenden Verkehrs in den Parkraumbewirtschaftungsgebieten von einer besonderen Dienststelle der Polizei wahrgenommen, die sich von der „normalen" Polizeibehörde nur darin unterscheidet, daß die Einnahmen und Ausgaben nicht im Haushaltsplan des Polizeipräsidenten sondern in einem gesonderten Wirtschaftsplan (§ 26 LHO) ausgewiesen werden. Die Bedenken des Datenschutzbeauftragten, daß es sich bei der Tätigkeit der Parkraumüberwacher der Polizei (es handelt sich um Angestellte im Verkehrsüberwachungsdienst) nicht um eine hoheitliche Aufgabenerfüllung handeln könne, sind nicht nachvollziehbar. Dies entspräche auch nicht der herrschenden Rechtsauffassung, die u.a. vom Kammergericht vertreten wird.

Nach Vertragsbeendigung werden bei den bisherigen Betreiberfirmen keine Daten mehr vorhanden sein, da die PC-Daten sofort nach Überspielung auf die der Bußgeldstelle beim Polizeipräsidenten in Berlin zu überbringenden Streamerbänder gelöscht werden. Es wird von der zuständigen Senatsverwaltung überprüft werden, daß sich keine entsprechenden Daten mehr auf den PCs der Firmen befinden. Nach Überspielung der letzten Daten werden die Streamerbänder beim Polizeipräsidenten verbleiben.

4.3 Zwei traditionelle Verwaltungen – Justiz und Finanzen

4.3.1 Justiz

Strafprozeßordnung

Die Diskussion um die Einführung des *„Großen Lauschangriffs"*, also der akustischen Überwachung von Wohnungen zur Strafverfolgung, ist fortgeführt worden. Ein Formulierungsentwurf des Bundesjustizministeriums zur Änderung von Art. 13 GG ist allerdings vom Entwurf eines Strafverfahrensänderungsgesetzes wieder abgekoppelt worden. Wir halten mit der Mehrheit der Datenschutzbeauftragten an der Auffassung fest, daß die Intensität des Eingriffs in diesem unantastbaren Bereich privater Lebensgestaltung in keinem akzeptablen Verhältnis zu dem zu erwartenden Ertrag für die Strafverfolgung steht[95].

Der Senat teilt die Auffassung, daß der Einsatz technischer Mittel zum Aufzeichnen oder Abhören von Gesprächen innerhalb des durch Art. 13 GG geschützten Bereichs einen besonders intensiven Eingriff in die Kommunikationsfreiheit und das Persönlichkeitsrecht des Betroffenen darstellt. Da im Bereich der Ermittlungstätigkeit wegen begangener Straftaten die Unschuldsvermutung gewahrt bleiben muß, wird der Senat Überlegungen zu gesetzlichen Regelungen nur nähertreten, wenn sie in sachlicher wie verfahrensrechtlicher Hinsicht größtmögliche Garantien gegen unverhältnismäßige Eingriffe in diese Rechte bieten.

Dabei ist jedoch auch zu bedenken, daß nach den in den USA gewonnenen Erfahrungen das elektronische Abhören das wichtigste taktische Einsatzmittel zur Bekämpfung schwerer Kriminalität ist. Für die Erforderlichkeit des „großen Lauschangriffs" spricht insbesondere die aus Ermittlungsverfahren gewonnen Erkenntnis, daß sich Straftäter längst auf die für die Strafverfolgungsbehörden nach geltendem Recht sehr eng begrenzten Einsatzmöglichkeiten von Abhörtechnik eingestellt haben. Für die Verabredung und Durchführung von Straftaten der Schwerkriminalität werden zunehmend Wohnungen und gleichgestellte Räumlichkeiten (Hotelzimmer, Büros usw.) benutzt.

Die Möglichkeit einer akustischen Überwachung in Wohnungen kann zwar nicht verhindern, daß die Täter ihre konspirativen Gespräche künftig an anderen Orten führen.

[95] JB 1992, 4.2.1

Außerhalb von Wohnungen ist den Ermittlungsbehörden eine Überwachung derartiger Gespräche aber bereits jetzt rechtlich möglich. Deshalb ist die Einführung des „großen Lauschangriffs“ geeignet, den Freiraum für Straftäter entscheidend einzuengen und die Möglichkeit einer Aufklärung und Verfolgung von Straftaten, die Gegenstand solcher Gespräche sind, wirksam zu verbessern.

Eine ähnlich wirksame Alternative gibt es nicht. Der Einsatz von verdeckten Ermittlern und Vertrauenspersonen ist gerade im Bereich der Schwerkriminalität wegen des hohen Anteils ausländischer Täter und der damit einhergehenden Abschottung von Tätergruppen schwierig und nicht geeignet, technische Mittel zu ersetzen.

Hierzu ist ein Urteil des *Sächsischen Verfassungsgerichtshofes*[96] bemerkenswert, das sich mit einer Regelung im Sächsischen Polizeigesetz über den Lauschangriff zur Gefahrenabwehr auseinandergesetzt hat. Dieser ist mit der Sächsischen Verfassung nur dann vereinbar, wenn er zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leben, Gesundheit und Freiheit einer Person oder für bedeutende fremde Sach- oder Vermögenswerte erforderlich ist. Er darf sich darüber hinaus nur gegen für die Gefahr Verantwortliche und nicht gegen Dritte richten.

Der Lauschangriff darf ferner nicht den *absolut geschützten Bereich privater Lebensführung* betreffen. Jeder Mensch muß Räume haben, in die er sich zurückziehen kann und in denen er von der Obrigkeit völlig in Ruhe gelassen wird. Jeder Mensch hat einen Anspruch auf Schutz seiner privaten Intimsphäre. Das Gericht hat festgestellt, daß in diesem Bereich auch schwerwiegende Interessen der Allgemeinheit oder gar Einzelner einen staatlichen Eingriff nicht zu rechtfertigen vermögen. Sollte sich erst nach einer geplanten Abhörmaßnahme herausstellen, daß der absolut geschützte Bereich privater Lebensführung von der Abhörmaßnahme betroffen worden ist, so sind die Aufzeichnungen unverzüglich zu löschen.

Strafverfahrensänderungsgesetz: Ein neuer Gesetzentwurf

Am Ende des Jahres 1996 – sozusagen als Weihnachtsüberraschung – hat die Bundesregierung nunmehr einen eigenen Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1996 – (StVÄG 1996) vorgelegt[97].

Leider wird auch der von der Bundesregierung vorgelegte Gesetzentwurf in weiten Teilen den Vorgaben des Bundesverfassungsgerichtes[98], Eingriffe in das Recht auf informationelle Selbstbestimmung durch den Gesetzgeber präzise und umfassend zu regeln, nicht gerecht.

Nach § 163 f. des Gesetzentwurfes soll in Zukunft bei „zureichenden tatsächlichen Anhaltspunkten dafür, daß eine Straftat von erheblicher Bedeutung begangen worden ist”, eine planmäßig angelegte *Beobachtung von Beschuldigten durchgehend länger als 24 Stunden* oder an mehr als zwei Tagen angeordnet werden dürfen. Voraussetzung ist, daß die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die Observation darf sich auch gegen Dritte richten. Bei Gefahr im Verzug darf die Anordnung von der Staatsanwaltschaft oder ihren Hilfsbeamten (der

Zur grundsätzlichen Problematik der Ausgestaltung datenschutzrechtlicher Grundsätze im Bereich des Strafverfahrens wird zunächst auf die Stellungnahme zu Ziff. 1.1 des Berichts verwiesen. Zu dem Entwurf eines Strafverfahrensänderungsgesetzes 96 hat der Bundesrat am 21. Februar 1997 eine Stellungnahme gegenüber der Bundesregierung abgegeben.

Der Entwurf betrifft eine Vielzahl von Regelungen mit datenschutzrechtlichem Bezug. Zu Einzelfragen kann wegen der laufenden Beratungen zum jetzigen Zeitpunkt keine Stellungnahme abgegeben werden. Grundsätzlich ist der Entwurf zu begrüßen, da er für verschiedene Formen des Eingriffs in die informationelle Selbstbestimmung eine Rechtsgrundlage zur Verfügung stellt und Umfang und Art zulässiger Eingriffe konkretisiert. Wegen der Vielgestaltigkeit polizeilicher und staatsanwaltschaftlicher Ermittlungsmaßnahmen sind die Regelungen notwendigerweise zum Teil generalklauselartig gefaßt. Ferner ist im Bereich der Datenverarbeitung und im Auskunftswesen zu berücksichtigen, daß mit angemessenem Verwaltungsaufwand eine gute Effizienz bei gleichzeitig größtmöglichem Schutz des Betroffenen zu erreichen ist. Der Senat setzt sich bei den Beratungen jeweils auf der Grundlage der vom „Volkszählungsurteil“ vorgegebenen Maßstäbe für einen

[96] Sächsischer VerfGH, Urt. v. 14. Mai 1996, Vf. 44 – II – 94
[97] BR-Drs. 961/96; s.a. BR-Drs. 620/94 vom 14. Oktober 1994 (StVÄG-Entwurf der Länder), JB 1993, 4.7; JB 1994, 4.8
[98] BVerfGE 65, 1, 44

Polizei) getroffen werden.

Diese Regelung ist in vielen Punkten zu unbestimmt. Der Gesetzgeber sollte eine bestimmte Schwelle des Verdachtes für erforderlich erklären. Die Straftaten, die erheblich sein können, sind im Gesetz konkret zu benennen. Zu unpräzise ist die Voraussetzung, daß die Erforschung des Sachverhaltes ohne die Observation „wesentlich erschwert" wäre. Sie sollte vielmehr zur Aufklärung weiterer Straftaten erforderlich sein. Observierung von Dritten sollte an qualifizierte Voraussetzungen geknüpft werden. Wegen der Schwere des Eingriffes halten wir eine Anordnung der Observation nur durch die Polizei für unangemessen.

Die §§ 474 ff. des Entwurfes regeln die *Erteilung von Auskünften und Akteneinsichten* aus den Verfahrensakten. Auch diese Regelungen enthalten eine Vielzahl unbestimmter Rechtsbegriffe, die dem Gebot der Normenklarheit nicht gerecht werden. Ein wesentlicher Kritikpunkt ist die nicht ausreichende Unterscheidung zwischen Daten über Beschuldigte, Verdächtige und andere Personen. Problematisch ist auch eine Regelung, nach der Akteneinsicht gewährt werden kann, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordert. Es besteht die Gefahr, daß bei Auskunftsersuchen von Justizbehörden oder öffentlichen Stellen unter Hinweis auf den Aufwand die ganze Akte übersandt wird.

Der Gesetzentwurf sieht auch vor, durch die Errichtung eines *automatisierten Verfahrens* verschiedenen öffentlichen Stellen direkten Zugriff auf eine Vielzahl von höchst sensiblen Daten zu gewähren. Die Regelung ist um so bedenklicher, als sie keine klaren Festlegungen in bezug auf die zugriffsberechtigten Stellen, den abzurufenden Datenumfang und die Verwendungszwecke der Daten enthält.

Wir haben nur einige Punkte aus dem langen Katalog an datenschutzrelevanten Regelungen des Gesetzentwurfes aufgegriffen. Sie zeigen jedoch exemplarisch das eingangs dargestellte Problem, daß es den Regelungen an der erforderlichen Normenklarheit fehlt. Statt dessen lassen die Regelungen auch für die Zukunft Spielraum für Unsicherheiten sowohl bei den Gesetzesvollziehern als auch bei den von den Grundrechtseingriffen betroffenen Personen bei der Auslegung der Vorschriften.

weitgehenden Ausgleich der Interessen ein. Die Stellungnahme des Berliner Datenschutzbeauftragten findet hierbei selbstverständlich Berücksichtigung.

Genetische Informationen im Strafprozeß

Der Bundestag hat Anfang Dezember 1996 restriktive Regelungen zur Nutzung von genetischen Informationen im Strafprozeß beschlossen[99], über die bereits seit mehreren Jahren diskutiert worden ist[100]. In der Strafprozeßordnung wird jetzt eindeutig klargestellt, daß Blutproben oder sonstige Körperzellen, die dem Beschuldigten entnommen werden, nur für das zugrundeliegende Strafverfahren oder ein anderes gegenwärtig anhängiges Strafverfahren verwendet werden dürfen und sofort vernichtet werden müssen, wenn sie hierfür nicht mehr erforderlich sind. Eine Sammlung von Blutproben oder Körperzellen für zukünftige Strafverfahren wird damit ausgeschlossen. *Molekulargenetische Untersuchungen* dürfen ausschließlich zur Feststellung der Abstammung oder zur Klärung der Frage durchgeführt werden, ob Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt, und dies auch nur, wenn der Beschuldigte nicht auf andere Weise überführt werden kann. Entscheidend ist die Festlegung des Gesetzgebers, daß darüber hinausgehende Informationen, etwa über äußere Merkmale oder Anlagen zu Krankheiten, im Strafprozeß nicht mit molekulargenetischen Methoden erhoben und verwendet

Der Senat begrüßt ebenfalls die Verabschiedung der Neuregelungen in §§ 81 a ff. StPO zur DNA-Analyse zu strafprozessualen Zwecken (sog. „genetischer Fingerabdruck"). Gerade angesichts fortschreitender Möglichkeiten in der Analysetechnik ist eine gesetzliche Begrenzung der Untersuchung im Rahmen der Strafverfolgung auf bestimmte Zwecke erforderlich. Hierüber bestand in Bundestag und Bundesrat eine weitgehende Einigkeit.

[99] BT-Drs. 13/667; BR-Drs. 5/97
[100] vgl. JB 1993, 4.7

werden dürfen. Derartige *Überschußinformationen* fallen zwar nach dem gegenwärtigen Erkenntnisstand bei der Erstellung eines *„genetischen Fingerabdrucks"* nicht an, weil ausschließlich ein Bereich des menschlichen Genoms untersucht wird, der als „nicht-sprechend" angesehen wird. Dies kann sich jedoch angesichts der weltweit mit hohem finanziellem Aufwand betriebenen Entschlüsselung des gesamten menschlichen Genoms durchaus in naher Zukunft ändern. Deshalb hat der Gesetzgeber ein ausdrückliches Verbot zur Erhebung und Verwertung von Überschußinformationen in die Strafprozeßordnung aufgenommen.

Genetische Untersuchungen dürfen ohnehin nur durch den Richter angeordnet werden, der auch den Sachverständigen zu bestimmen hat. Gehört der Sachverständige der Polizei an, so muß er in einer Organisationseinheit der Polizei tätig sein, die von der ermittlungsführenden Dienststelle organisatorisch und sachlich getrennt ist. Dem Sachverständigen ist das Untersuchungs- und Spurenmaterial ohne Namen, Anschrift und Geburtsdatum des Betroffenen zu übergeben. Der Berliner Datenschutzbeauftragte hat die Einhaltung dieser Schutzvorkehrungen von Amts wegen bei Untersuchungen zu überwachen, die in Berlin von öffentlichen oder privaten Stellen auf richterliche Anordnung durchgeführt werden.

Justizmitteilungsgesetz

Im letzten Jahresbericht[101] hatten wir darüber berichtet, daß die Bundesregierung Ende des Jahres noch den längst überfälligen Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz)[102] vorgelegt hatte. Die von den Datenschutzbeauftragten angeregten Änderungen sind bisher leider im Gesetzgebungsverfahren nicht aufgegriffen worden. Der Bundesrat hat in seiner Stellungnahme zu dem Gesetzentwurf der Bundesregierung zu vielen Punkten Vorschläge unterbreitet, die auf eine Verringerung des Aufwandes für die Justiz abzielen. So strebt der Bundesrat beispielsweise eine Beschränkung der Prüfung der Datenübermittlungen durch die übermittelnde Stelle auf eine reine Schlüssigkeitsprüfung an. In der Praxis könnten danach personenbezogene Daten auch ohne eine vorherige Prüfung der Erforderlichkeit der Daten für die Aufgabenerfüllung einer anderen Behörde übermittelt werden. Dies ist nur einer von zahlreichen Änderungswünschen des Bundesrates. Inwieweit der Bundesrat diese Änderungen durchsetzen kann, ist noch offen.

Der Senat sieht ein dringendes Bedürfnis für die baldige Verabschiedung des in den Beratungen befindlichen Entwurfs zu einem Justizmitteilungsgesetz. Angesichts der laufenden Gesetzberatungen enthält sich der Senat einer Bewertung der Entwürfe im einzelnen.

Korruptionsbekämpfung in Berlin

Zur Bekämpfung der Korruption in der Berliner Verwaltung plant die Senatsverwaltung für Justiz ein Gesetz über die Einrichtung einer *Zentralen Erfassungs- und Koordinierungsstelle zur Vorbeugung gegen Korruptionstaten* in Berlin.

Nach den Vorstellungen der Justizverwaltung sollen alle Dienstkräfte des Landes Berlin verpflichtet werden, Hinweise oder tatsächliche Anhaltspunkte, die auf Korruption in der Verwaltung hindeuten, ohne Einschaltung des Dienstweges an diese Stelle zu *melden*. Die Koordinierungsstelle soll diese Hinweise und Meldungen dann prüfen und ggf. unter Einschaltung weiterer Stellen wie dem Rechnungshof oder der Innenrevision der betroffenen Verwaltung den Sachverhalt aufklären. Wenn die Koordinierungsstelle zu dem Schluß kommen sollte, daß Anhaltspunkte für eine Straftat vorliegen, soll sie die Strafverfolgungsbehörden einschalten.

[101] JB 1995, 5.7
[102] BT-Drs. 12/1399

Es ist geplant, die Mitarbeiter des öffentlichen Dienstes, bei denen nach Auffassung der Koordinierungsstelle ein tatsächlicher Korruptionsverdacht besteht, in einer *besonderen Datei* zu speichern. Eine Benachrichtigungspflicht über die Speicherung in dieser Datei ist nicht vorgesehen; auch eine Löschungsfrist ist bisher nicht geplant – wenn man davon absieht, daß bei Wegfall des Korruptionsverdachtes die Daten gelöscht werden sollen.

Auch wir begrüßen die Absicht, Maßnahmen zur Bekämpfung der Korruption in der öffentlichen Verwaltung zu ergreifen. Allerdings bestehen gegen das bisher bekanntgewordene Konzept erhebliche datenschutzrechtliche Bedenken. Bei der beabsichtigten gesetzlichen Verpflichtung zur Meldung von Hinweisen oder tatsächlichen Anhaltspunkten für Korruption wird die Datenverarbeitung weit in das Vorfeld einer konkreten Gefahr oder eines Anfangsverdachtes verlagert. Sie erfolgt zudem hinter dem Rücken des Betroffenen.

Die Tätigkeit der Koordinierungsstelle läßt sich weder klar von der Tätigkeit der Polizei zur vorbeugenden Verbrechensbekämpfung noch von der Tätigkeit der Staatsanwaltschaft bei der Einleitung eines staatsanwaltschaftlichen Ermittlungsverfahrens abgrenzen. Für den Bereich der vorbeugenden Verbrechensbekämpfung enthält bereits das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG) Regelungen. Nach dem ASOG ist zudem allein die Polizei im Rahmen der Gefahrenabwehr für die vorbeugende Straftatenbekämpfung zuständig. Die Koordinierungsstelle soll dennoch neben der Polizei eigene Befugnisse zur vorbeugenden Straftatenbekämpfung erhalten, ohne allerdings den einschränkenden Voraussetzungen des ASOG zu unterliegen.

Mit der Befugnis der Koordinierungsstelle, über eine Weiterleitung der Hinweise und Meldungen an die Staatsanwaltschaft zur Einleitung eines Ermittlungsverfahrens zu entscheiden, würde der Entscheidungsspielraum der Staatsanwaltschaft, die Entscheidung zu treffen, ob ein Anfangsverdacht für eine Straftat überhaupt vorliegt, zum Teil bereits auf die Koordinierungsstelle vorverlagert. Damit würde der Staatsanwaltschaft in bestimmten Fällen die Möglichkeit genommen, gemäß § 160 Abs. 2 StPO selbst die be- und entlastenden Umstände jedes Einzelfalles zu ermitteln.

Ein weiterer Kritikpunkt ist die *fehlende Unterrichtung* der von Speicherungen betroffenen Mitarbeiter über die Tatsache, daß sie in einer besonderen Korruptionsdatei gespeichert sind. Nach § 16 Abs. 2 BlnDSG ist der Betroffene bei einer Speicherung in einer Datei grundsätzlich über die Speicherung zu unterrichten. Auch für die *Löschung* der gespeicherten Daten fehlen bisher Vorstellungen darüber, wann eine Löschung zu erfolgen hat oder in welchen Abständen die Voraussetzungen für eine Speicherung zumindest überprüft werden.

Der Gesetzentwurf wird derzeit unter Berücksichtigung der geltend gemachten Bedenken einer Überarbeitung unterzogen.

Bescheidung des Antragstellers nach Einstellung des Verfahrens gemäß §154 StPO

Ein Bürger beschwerte sich darüber, daß die Amtsanwaltschaft dem Anzeigeerstatter, aufgrund dessen Anzeige ein Ermittlungsverfahren eingeleitet worden war, in der Mitteilung über die Einstellung des Verfahrens nach § 154 StPO mitgeteilt hatte, unter welchem Aktenzeichen und bei welchem Gericht Ermittlungsverfahren gegen seine Person laufen, aus denen eine höhere Strafe zu erwarten sei, gegen die die aus dem eingestellten Ermittlungsverfahren zu erwartende Strafe nicht erheblich ins Gewicht falle.

Die Mitteilung des Aktenzeichens im Einstellungsbescheid an den Anzeigeerstatter ist nicht erforderlich. Allerdings sehen wir auch, daß der Einstellungsbescheid nachvollziehbar sein muß. Da offensichtlich auch die Justizverwaltung die Übermittlung

Aufgrund der Korrespondenz mit dem Berliner Datenschutzbeauftragten und nach Abstimmung der Behördenleiter verwendet die Staatsanwaltschaft nunmehr ein einheitliches Anschreiben bei Einstellungen gemäß § 154 StPO, in dem der

dieses Datums für nicht ganz unproblematisch hielt, sollte im Rahmen der Überarbeitung der Einstellungsformulare eine Änderung vorgenommen werden. Das uns übersandte überarbeitete Einstellungsformular enthält nun zwar nicht mehr die Angaben des Aktenzeichens, dafür jedoch eine Angabe des Tatvorwurfes. Damit ist aus datenschutzrechtlicher Sicht eine Verschlechterung eingetreten, da der Tatvorwurf ein noch sensibleres Datum ist, das bisher durch das Aktenzeichen allein nicht erkennbar war.

betreffende Tatvorwurf, angesichts dessen die zu erwartende Sanktion in dem angezeigten Verfahren nicht beträchtlich ins Gewicht fällt, bezeichnet wird. Gemäß § 171 Abs. 1 StPO ist ein Einstellungsbescheid mit Gründen zu versehen, die die Entscheidung aus sich selbst heraus verständlich und nachvollziehbar machen und dem Empfänger ein Abwägen ermöglichen, ob er den Bescheid anfechten oder hinnehmen will. Dieser im öffentlichen Recht allgemein geltende Grundsatz ist auch auf den über eine Einstellung des Verfahrens gemäß § 154 Abs. 1 StPO zu erteilenden Bescheid anzuwenden. Der in diesem Zusammenhang von Berliner Datenschutzbeauftragten gemachte Vorschlag, lediglich mitzuteilen, „daß gegen den Beschuldigten in einem oder mehreren bei dem Amtsgericht .../Landgericht ... geführten Verfahren eine höhere Strafe zu erwarten ist, gegen die die Strafe, zu der die Verfolgung im angezeigten Fall führen könnte, nicht beträchtlich ins Gewicht fallen würde“, wird dem nicht hinreichend gerecht. Die Staatsanwaltschaft wird diesen Vorschlag daher nicht aufgreifen.

Die Lotterie der Datenlöschung nach abgeschlossenem Ermittlungsverfahren

Gegen einen Petenten und mehrere Beteiligte wurde 1987 ein gemeinsames Ermittlungsverfahren eingeleitet. Das Ermittlungsverfahren gegen den Petenten wurde 1990 eingestellt. Die anderen verbundenen Verfahren waren auch 1995 noch nicht abgeschlossen. Da die fünfjährige Aufbewahrungsfrist für eingestellte Ermittlungsverfahren erst am Ende des Jahres zu laufen beginnt, in dem der Staatsanwalt die Abschlußverfügung in dem Ermittlungsverfahren vorgenommen hat, waren die personenbezogenen Daten des Petenten auch 1995 noch nicht gelöscht. Die Aufbewahrungsfrist hatte noch nicht einmal zu laufen begonnen.

Der beschriebene Fall zeigt eindrucksvoll, daß es dann nicht mehr nur auf die Länge einer Aufbewahrungsfrist ankommt, wenn sie durch den Zeitpunkt des „Ingangsetzens” variabel ist. Die Aufbewahrungsfrist hat sich im vorliegenden Fall verdoppelt.

Um in den Fällen eines *verbundenen Ermittlungsverfahrens*, in denen gegen mehrere Beschuldigte ermittelt wird, eine unzumutbare Verlängerung der Speicherung nach Abschluß des Ermittlungsverfahrens zu verhindern, sollte die Speicherfrist bei jedem Mittäter gesondert errechnet und entsprechend auch getrennte Weglegeverfügungen getroffen werden. Sowohl die Abtrennung der verbundenen Verfahren wäre ein Lösungsansatz als auch eine gesonderte Löschung der Daten im Vorgangsverwaltungssystem AStA (ADV-Verfahren Amts- und Staatsanwaltschaft) nach Ablauf der individuellen, für jeden einzelnen Mittäter berechneten Aufbewahrungsfrist. Auf diese Weise wäre zumindest ein unbefugter, landesweiter Zugriff auf die Daten ausgeschlossen, und die Akte könnte in den verbundenen Verfahren noch herangezogen werden.

Leider hat die Staatsanwaltschaft unsere Vorschläge abgelehnt. Eine individuelle Löschungsfrist im AStA-System wurde unter Hinweis auf die Aufgabe des AStA-Systems, als Vorgangsverwaltungssytem den Zugang zu den Akten zu ermöglichen, abgelehnt. Eine Trennung der verbundenen Ermittlungsverfahren wird aus Verfahrensgründen offensichtlich auch nicht für möglich gehalten. In diesen Fällen bleibt offensichtlich bei der Frage der Speicherfrist nur das „Prinzip Zufall”.

Zutreffend weist der Berliner Datenschutzbeauftragte auf die beschränkte Funktion des ASTA-Systems als bloßes Vorgangsverwaltungssystem zur Ermöglichung des Zugangs zu den Akten hin. Wie die früheren papierenen Register und Namenskarteien hat ASTA die Aufgabe, den schnellen und einfachen Zugriff auf den Aktenbestand zu ermöglichen, um den Berechtigten Auskunft über Verfahren, Verfahrensbeteiligte und -stände erteilen zu können. Die ASTA-Auskunft ist dabei lediglich ein Findhinweis, rechtlich und tatsächlich maßgebend für die Auskünfte ist allein der jeweilige Akteninhalt.

Unzutreffend dagegen ist die Darstellung des Berliner Datenschutzbeauftragten, daß die Dauer der Speicherfrist von Personendaten vom Zufall abhängig sei. Auch in Fällen wie dem im Bericht dargelegten ist die Frage, ob mehrere Beschuldigte in einem Verfahren geführt werden, nicht vom Zufall abhängig, sondern durch den zu ermittelnden strafrechtlich relevanten Sachverhalt von vornherein vorgegeben oder aus prozeßökonomischen Gesichtspunkten (vgl. Nr. 114 RiStBV) nicht zuletzt im Interesse der Beschuldigten erforderlich. Da es für eine gerechte Beurteilung eines jeden Mitbeschuldigten unerläßlich ist, daß seine Stellung im gesamten Verfahren sichtbar wird, gibt es keinen strafprozessualen Rechtssatz, der die Abtrennung eingestellter Verfahrensteile gebietet.

Nach den Erfahrungen der staatsanwaltschaftlichen Praxis kommt es im übrigen häufig vor, daß Anträge und Auskunftsersuchen sich auf lange zurückliegende Verfahren und Sachverhalte beziehen. Es wäre nicht verständlich, wenn derartigen Anliegen – bei Berechtigung – trotz der Existenz der Akte nicht nachgegangen werden könnte, weil eine Zuordnung der Akte wegen bereits gelöschter Personaldaten des

Betroffenen nicht möglich ist.

Die angeregte individuelle Löschungsfrist in ASTA würde dessen Aufgabe als bloßes Vorgangsverwaltungssystem zuwiderlaufen und zu einem nicht zu vertretenden Auseinanderlaufen von Aktenbestand und Aktendatenbestand führen.

Die offenbarte Inkognito-Adoption

Die leiblichen Eltern eines inkognito-adoptierten Kindes erhielten viele Jahre nach der Adoption einen Anruf einer Schwester des adoptierten Kindes, die erklärte, die Informationen über die Inkognito-Adoption ihrer Schwester vom damals für das Adoptionsverfahren zuständigen Gericht erhalten zu haben. Sie habe Einsicht in die Adoptionsunterlagen aller Geschwister nehmen können und besitze von diesen Unterlagen jetzt auch Kopien.

Bei Inkognito-Adoptionen wird nach § 61 Personenstandsgesetz ein Sperrvermerk eingetragen. Wenn Einsichtnahme in die Adoptionsunterlagen begehrt wird, entscheidet hierüber der zuständige Vormundschaftsrichter nach § 1758 Bürgerliches Gesetzbuch (BGB) i.V.m. § 34 Abs. 2 Gesetz über die freiwillige Gerichtsbarkeit (FGG). Es handelt sich um eine Entscheidung im Bereich der richterlichen Unabhängigkeit, der nach § 24 Abs. 2 BlnDSG unserer Kontrollkompetenz entzogen ist. Es gehört jedoch zu unseren Aufgaben aufzuzeigen, welche datenschutzrechtlichen Probleme auch in diesem Bereich auftreten können:

Nach § 1758 Abs. 1 BGB dürfen bei Inkognito-Adoptionen Tatsachen, die geeignet sind, die Adoption und ihre Umstände aufzudecken, ohne Zustimmung des Annehmenden und des Kindes nicht offenbart oder ausgeforscht werden, es sei denn, daß besondere Gründe des öffentlichen Interesses dies erfordern. Sinn und Zweck dieser Auskunftsbeschränkung ist die Geheimhaltung der Adoption. Im vorliegenden Fall konnte nicht ausgeschlossen werden, daß bei der Durchsicht der Akten zur Vorbereitung der Entscheidung über die beantragte Akteneinsicht übersehen worden war, daß es sich um eine Inkognito-Adoption gehandelt hat. Wie auch immer dieser von der Senatsverwaltung für Justiz als Sachverhaltsirrtum bezeichnete Irrtum zustande gekommen ist – die Übermittlung der Adoptionsdaten entgegen der Vorschrift des § 1758 BGB steht im Ergebnis fest und ist in diesen Fällen nicht mehr rückgängig zu machen. Die Inkognito-Adoption ist nun auch Dritten bekannt, und die Familie des betroffenen Kindes muß mit den Folgen leben.

Die Darstellung weist zutreffend darauf hin, daß es sich bei der Einsichtnahme in die Adoptionsunterlagen um eine Entscheidung handelt, die in richterlicher Unabhängigkeit getroffen wird und somit der Kontrollkompetenz des Berliner Datenschutzbeauftragten entzogen ist. Angesichts der Tatsache, daß es sich um einen auf einem Sachverhaltsirrtum beruhenden Einzelfall handelt, sieht der Senat keinen weiteren Erörterungsbedarf.

Übersendung von vollständigen Grundbuchauszügen bei Umschreibungen des Grundbuches auf ein Lose-Blatt-Grundbuch

Ein Bürger mußte nach dem Kauf eines Hauses und seiner Eintragung als neuer Eigentümer im Grundbuch feststellen, daß das zuständige Grundbuchamt seinen neuen Nachbarn, die dinglich Berechtigte waren, im Zuge der Umschreibung des Grundbuches neben Auszügen aus den Abteilungen I und II des Grundbuches auch Auszüge der Eintragungen in der Abteilung III mit den hypothekarischen Belastungen des Grundstückes übermittelt hatte.

Die Benachrichtigungspflicht der dinglich Berechtigten ergibt sich aus § 55 Grundbuchordnung (GBO) i.V.m. § 39 Abs. 3 Grundbuchverfügung (GBVfg). Bei Umschreibungen eines Grundbuchblattes ist den dinglich Berechtigten die Umschreibung bekanntzugeben. Soweit mit der Umschreibung keine Änderung der Rangverhältnisse in den Grundbuchabteilungen verbunden ist, genügt es nach unserer Auffassung, dem dinglich Berechtigten nur die Umschreibung mitzuteilen und ihm zur Ermöglichung der Überprüfung einer ordnungsgemäßen

Die Auslegung und Anwendung der Vorschriften der Grundbuchordnung und der Grundbuchverfügung obliegt dem Rechtspfleger, dem im Hinblick auf seine sachliche Unabhängigkeit nach § 9 Rechtspflegergesetz keine Weisungen über das Verfahren gegeben werden können. Es handelt sich mithin um eine Angelegenheit, die gemäß § 24 Abs. 2 Satz 1 Berliner Datenschutzgesetz der Kontrollbefugnis des Datenschutzbeauftragten entzogen ist.

Die Senatsverwaltung für Justiz konnte sich dennoch der An-

Übertragung seines Rechtes Auszüge der Abteilungen zu übersenden, wobei in der Abteilung II die Angabe der Rangposition seines Rechtes ausreichen dürfte. Die Höhe der hypothekarischen Belastungen spielt für den dinglich Berechtigten keine Rolle.

Die Senatsverwaltung für Justiz hat – auch wenn sie Zweifel an unserer Kontrollkompetenz in diesen Grundbuchfällen hat – die Grundbuchämter gebeten, bei ihren Ermessensentscheidungen hinsichtlich der Datenübermittlungen an dinglich Berechtigte immer auch die datenschutzrechtlichen Belange der Betroffenen in die Überlegungen einzubeziehen. Diese Empfehlung an die Grundstücksämter wird hoffentlich zu einem sensibleren Umgang mit Grundbuchauszügen führen.

sicht nicht verschließen, daß die Übersendung vollständiger Grundbuchauszüge an alle in der zweiten und dritten Abteilung des Grundbuchs eingetragenen Berechtigten zum Zwecke der Benachrichtigung nicht erforderlich ist. An der Höhe der hypothekarischen Belastungen des Eigentümers hat der Dienstbarkeitsberechtigte, soweit ersichtlich, kein rechtliches Interesse.

Unabhängig von der Möglichkeit, daß Dienstbarkeitsberechtigte nach § 12 Grundbuchordnung Grundbucheinsicht nehmen und somit auf Antrag jederzeit entsprechende Informationen erhalten können, hat die Senatsverwaltung für Justiz den Grundbuchrechtspflegern zu Bedenken gegeben, daß bei der vom Rechtspfleger von Amts wegen in sachlicher Unabhängigkeit zu treffenden Entscheidung auch die datenschutzrechtlichen Belange der Eigentümer Berücksichtigung finden sollten.

4.3.2 Finanzen

Über die bedauerliche Situation hinsichtlich der spezialrechtlichen Regelung des Datenschutzes in der Abgabenordnung wurde oben schon berichtet[103].

Der Senat verweist auf seine Stellungnahme zu Ziffer 1.1, „Deutschland und Europa“ („Informationelle Selbstbestimmung – ein alter Hut?“)

Vermögensrechtsdatenverarbeitungsgesetz – eine Frist soll verlängert werden

Die Senatsverwaltung für Finanzen hat Ende des Jahres einen Entwurf zur Änderung des im letzten Jahr in Kraft getretenen Vermögensrechtsdatenverarbeitungsgesetzes (VermDVG) in das Abgeordnetenhaus eingebracht. Sie will die Frist für eine Übergangsphase bis zum 31. Dezember 1996 für ein automatisiertes Abrufverfahren personenbezogener Daten durch die Fach- und Rechtsaufsichtsbehörde zur Durchführung des Vermögensgesetzes und des Lastenausgleichsgesetzes um zwei Jahre verlängern.

Bereits im Gesetzgebungsverfahren hatten wir kritisiert, daß derartige Online-Zugriffe zugelassen werden sollten. Wir sind der Auffassung, daß bei *Fach- und Rechtsaufsichtsbehörden* ein automatisiertes Abrufverfahren bei der kontrollierten Behörde nicht angemessen ist (§ 15 Abs. 1 BlnDSG). Um wenigstens eine Kontrolle der Abrufe zu ermöglichen, hat der Gesetzgeber eine Protokollierung der Abrufe zwingend vorgeschrieben.

Bei einer Prüfung der technisch-organisatorischen Maßnahmen bei dem Abrufverfahren haben wir festgestellt, daß die in § 3 Abs. 2 VermDVG sowie in § 5 Abs. 3 Nr. 6 BlnDSG vorgeschriebene *Protokollierung der einzelnen Abrufe* in der Vergangenheit nicht erfolgt ist und aus technischen Gründen auch bei einer Verlängerung der Frist im VermDVG in Zukunft nicht erfolgen kann. Die Protokollierung ermöglicht jedoch zum einen eine Überprüfung der Erforderlichkeit eines automatisierten Abrufverfahrens, zum anderen können durch eine Protokollierung mißbräuchliche Abrufe aufgedeckt werden.

Die in § 3 Abs. 2 VermDVG vorgesehene Rechtsverordnung, die bei automatisierten Abrufverfahren auch nach § 15 Abs. 2 BlnDSG zwingend vorgeschrieben ist, ist bisher nicht erlassen worden. Sie ist auch nicht in Vorbereitung.

Die Verlängerung der Frist für ein automatisiertes Abrufverfahren entbehrt damit jeder Grundlage.

Vor dem Hintergrund eines auf dem Gebiet der Bürokommunikation einmaligen Projektes zur Vorgangsbearbeitung, VERADOK, wurde zum Zeitpunkt des Inkrafttretens des VermDVG der Fach- und Rechtsaufsichtsbehörde der automatische Abruf befristet erlaubt. Angesichts des ungeklärten Projektfortganges und offener Realisierungsfragen wurde eine Gesetzesänderung zur Verlängerung der Frist eingebracht, aufgrund der Bedenken des Berliner Datenschutzbeauftragten zwischenzeitlich aber zurückgezogen.

Aufgrund des Wegfalls der Rechtsgrundlage wurde der Online-Zugriff auf personenbezogene Daten des VERADOK-Systems durch die für die Fach- und Rechtsaufsicht zuständigen Bereiche der Senatsverwaltung für Finanzen zum 1. Januar 1997 eingestellt. Die entsprechenden Zugriffskennungen sind gelöscht worden. Eine Fristverlängerung zum § 3 Abs. 2 VermDVG und der Erlaß einer Rechtsverordnung nach § 3 Abs. 2 VermDVG sind somit nicht mehr notwendig.

Das Fahrtenbuch

Wer einen Dienstwagen nutzt, ist in der Regel verpflichtet, ein Fahrtenbuch zu führen, um bei der Steuererklärung die

[103] vgl. oben 1.1

betriebliche Veranlassung der durchgeführten Fahrten sowie den Anteil der privaten Nutzung des Dienstwagens nachweisen zu können. Im Fahrtenbuch sind u.a. der Name und die Anschrift des aufgesuchten Geschäftspartners einzutragen. Die bloße Angabe „Geschäftsfahrt" wird als nicht ausreichend angesehen.

Wir haben der Senatsverwaltung für Finanzen mitgeteilt, daß wir die Angabe „Geschäftsfahrt" als ausreichend ansehen. Sollten im Einzelfall Zweifel an der Richtigkeit der gemachten Angaben bestehen, hat die Finanzverwaltung nach § 93 Abs. 1 Abgabenordnung (AO) die Möglichkeit, den Steuerpflichtigen um nähere *Darlegung der Geschäftspartner* zu bitten, wobei dann auch private Aufzeichnungen etwa im Terminkalender genutzt werden könnten. Es würden dem Finanzamt nur dann Daten Dritter übermittelt, wenn dies im Einzelfall als Nachweis erforderlich ist. Bei der vom Bundesfinanzministerium geforderten detaillierten Führung eines Fahrtenbuches muß jeder, der in geschäftlichen Beziehungen mit einem Besitzer eines Dienstwagens steht, der diesen zu Geschäftsfahrten regelmäßig nutzt, damit rechnen, daß seine personenbezogenen Daten im Fahrtenbuch gespeichert werden und an die Finanzverwaltung übermittelt werden – und dies, obwohl keine gesetzliche Regelung für die Datenverarbeitung existiert. Die Senatsverwaltung für Finanzen hat sich unserem Vorschlag leider nicht angeschlossen, in Zukunft die Angabe „Geschäftsfahrt" genügen zu lassen. Sie verweist darauf, daß eine Überprüfung häufig erst Jahre später stattfinde und das Fahrtenbuch deshalb erforderlich sei.

Leider ist auch mit dem Jahressteuergesetz 1997 diese Form der Besteuerung beruflich genutzter Fahrzeuge trotz vieler Proteste nicht rückgängig gemacht worden.

Bei der Besteuerung beruflich genutzter Fahrzeuge handelt es sich um eine vom Steuergesetzgeber vorgegebene Regelung, deren verwaltungsmäßigem Vollzug sich Berlin nicht willkürlich entziehen kann.

Aus fachlicher Sicht wird auch weiterhin kein Gestaltungsspielraum gesehen, bei der Erfüllung des Gesetzesauftrags auf die in Rede stehenden Daten bei der Führung von Fahrtenbüchern zu verzichten. Das Fahrtenbuch hätte ohne die Angabe des aufgesuchten Geschäftspartners (Kunden/Klienten) nicht mehr den Charakter einer schlüssigen Dokumentation und wäre als Beweis für die betriebliche/berufliche Veranlassung der Fahrten ungeeignet.

Unzutreffend ist die Darstellung, daß der Dienstwagenbenutzer die im Fahrtenbuch enthaltenen Daten Dritter der Finanzverwaltung (laufend gespeichert) zu übermitteln habe. Zutreffend ist vielmehr, daß die Aufzeichnungen in einem Fahrtenbuch – nicht anders als ggf. zur Nachweisführung heranzuziehende private Aufzeichnungen in einem Terminkalender – in der Regel durch das Finanzamt (nur) im Rahmen von Betriebsprüfungen in den Räumen des Steuerpflichtigen eingesehen werden. Es ist nicht nachvollziehbar, daß Aufzeichnungen in einem Terminkalender datenrechtlich stärker geschützt sein sollten als die in einem Fahrtenbuch, zumal beide Kalendarien sowohl manuell als auch elektronisch geführt werden können.

Die Schmierpapier-Affäre

Ein Strafgefangener stellte bei seiner Arbeit in der Buchbinderei einer Justizvollzugsanstalt fest, daß es sich bei den Blättern, die er zu Notizblöcken binden sollte, um Auszahlungslisten eines Berliner Sozialamtes handelte. Auf den Auszahlungslisten waren Namen, Adressen und Kontonummern von Sozialleistungsempfängern vermerkt.

Was war passiert? Bei der Einführung des haushaltsrechtlichen Programmes *ProFISKAL* war es im Sozialamt eines Bezirksamtes zu Fehldrucken bei der Überprüfung der noch nicht freigegebenen Zahlungen gekommen. Diese Fehldrucke wurden gesondert gesammelt, um sie anschließend ordnungsgemäß zu vernichten. Da zu diesem Zeitpunkt auch Papier gesammelt wurde, aus dem anschließend in der Buchbinderei der Justizvollzugsanstalt Notizblöcke hergestellt werden sollten, konnte es passieren, daß ein Mitarbeiter versehentlich die Fehldrucke zur Notizblockverarbeitung gegriffen und weitergegeben hat. In der Buchbinderei war dies nicht aufgefallen, da sich der Stapel mit den Fehldrucken inmitten der eigentlichen „Schmierblätter" befand.

Das betroffene Bezirksamt hat uns versichert, daß es sich um einen absoluten Einzelfall gehandelt hat. Vorsorglich seien noch einmal alle Mitarbeiter auf ihre Sorgfaltspflicht im Umgang mit personenbezogenen Daten hingewiesen worden.

4.4 Selbstverwirklichung im Sozialstaat: Datenverarbeitung am Arbeitsplatz, im Gesundheitswesen, bei Bau und Wohnen

4.4.1 Arbeitnehmer und öffentliche Bedienstete

Aufnahme von Unterlagen in die Personalakte ohne Grenzen?

Eine ehemalige Bedienstete der Staatsanwaltschaft war an uns mit der Bitte um Prüfung ihrer Personalakte herangetreten. Bei einem Prüfbesuch im Personalamt stellten wir fest, daß sich in der Personalakte Vermerke des Vorgesetzten über Telefongespräche mit der Petentin befanden, die Einblick in die Intimsphäre und gesundheitliche Situation der Petentin während eines Krankenhausaufenthalts gaben, obwohl der Inhalt keinerlei Einfluß auf das Dienstverhältnis hatte.

Die Aufnahme des Vermerks über die psychische und körperliche Situation der Petentin in die Personalakte war unzulässig. Der Grundsatz der *Lückenlosigkeit und Vollständigkeit der Personalakte* muß dort seine *Grenzen* finden, wo es um die Intimsphäre geht. Weder der Schutz öffentlicher Interessen noch die Erhaltung der Funktionsfähigkeit des Personalaktenwesens erfordern die komplette Erfassung der persönlichen Verhältnisse jedes einzelnen Beschäftigten. Einen hergebrachten Grundsatz des Berufsbeamtentums, daß für Beamte etwas anderes gilt, gibt es nicht.

Wir haben das Vorgehen der Personalstelle beanstandet und um Entfernung dieser Vorgänge gebeten. Bei einem späteren Prüfbesuch stellte sich heraus, daß die beanstandeten Unterlagen sich nunmehr nicht mehr in der Hauptakte, sondern in *Nebenakten* befanden. Eine weitere Nebenakte enthielt den gesamten Schriftverkehr mit dem Berliner Datenschutzbeauftragten sowie Vermerke über dessen Besuch. Diese Vorgehensweise verstößt gegen § 51 Abs. 1 Landesbeamtengesetz (LBG), wonach nur solche Unterlagen in die Personalakte (Haupt- und Nebenakten) aufgenommen werden dürfen, die mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Denn die Nebenakten mit dem beanstandeten Inhalt würden die Petentin während ihrer Zugehörigkeit zum öffentlichen Dienst auch bei einer Versetzung stets „verfolgen" und beim neuen Dienstherren in entsprechend schlechtem Licht erscheinen lassen.

Unterlagen, die in keinem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen, sind nicht in die Personalakte aufzunehmen. Dabei kommt es in jedem Einzelfall auf den tatsächlichen Inhalt der Unterlage an. Soweit der Darstellung des Sachverhaltes zu entnehmen ist, liegen die Voraussetzungen für die Aufnahme in die Personalakte hier nicht vor. Ist ein Vorgang in die Personalakte gelangt, der inhaltlich nicht zu den Personalakten gehört, so ist er aus der Personalakte zu entfernen. Zur Personalakte gehören auch die Nebenakten. Für die Aufbewahrung des Schriftverkehrs mit dem Berliner Datenschutzbeauftragten gilt entsprechendes. Er ist daher in einer Sachakte aufzubewahren. Im übrigen sind Nebenakten nur Unterlagen, die sich auch in der Grund- oder in Teilakten befinden.

Die Aufbewahrung in Nebenakten war deshalb ebenfalls unzulässig.

Aufbewahrung von Personalakten

Eine Mitarbeiterin der Senatsverwaltung für Wirtschaft und Technik fand im Rahmen eines Arbeitsauftrags Unterlagen mit sensiblen personenbezogenen Daten über ihre Person in einem Aktenordner, der die Aufschrift „Referatsangelegenheiten" trug, im Schrank ihres Vorgesetzten vor. Da sie in der Form der Aufbewahrung dieser sensiblen Daten einen Verstoß gegen die geltenden Bestimmungen des Datenschutzes vermutete, wandte sie sich an den behördlichen Datenschutzbeauftragten, der seinerseits den Leiter der Personalabteilung informierte. Obwohl der Referatsleiter aufgrund dieses Vorfalls ein hausinternes Rundschreiben verfaßte, in dem die Aufbewahrung von personenbezogener Daten neu geregelt wurde, sah sich der Arbeitgeber in der Einsichtnahme in den Ordner einen groben Verstoß gegen die allgemeinen Dienstpflichten und mahnte die Beschäftigte ab.

Der Zugriff auf den Aktenordner und damit die Kenntnisnahme der darin enthaltenen Daten war nicht unbefugt, da er im Rahmen eines Arbeitsauftrags erfolgte. Rechtswidrig war vielmehr die Art der Aufbewahrung der personenbezogenen Daten. Bei der *Aufbewahrung nicht automatisiert verarbeiteter Daten*

Die Auffassung des Berliner Datenschutzbeauftragten wird hinsichtlich der Aufbewahrung von Personaldaten geteilt. Die Personalaktendaten sind vertraulich zu behandeln und vor unbefugter Einsicht zu schützen.

sind Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport oder der Vernichtung zu verhindern (§ 5 Abs. 2 BlnDSG). Da es sich bei den Daten darüber hinaus um Personalaktendaten im Sinne des § 56 LBG handelt, der entsprechend auch auf Angestellte im öffentlichen Dienst des Landes Berlin anzuwenden ist, trifft die Behörde eine gesteigerte Geheimhaltungspflicht, die zu einer besonders vertraulichen Behandlung und Vorkehrung gegen Mißbrauch zwingt.

Gegen diese Verpflichtung verstieß die Art der Aufbewahrung in erheblichem Maß. Die Tatsache, daß die Beschäftigte sich wegen des von ihr aufgedeckten Mißstandes zunächst an den behördlichen Datenschutzbeauftragten gewandt hat, belegte deren Pflichtbewußtsein dem Arbeitgeber gegenüber. Wir haben wegen der unsachgemäßen Aufbewahrung der Daten einen Mangel festgestellt und die Behörde aufgefordert, künftig einen sorgfältigen Umgang mit solchen personenbezogenen Daten zu pflegen sowie die förmliche Abmahnung zurückzunehmen.

Im konkreten Fall handelte es sich nicht um eine Personalakte, sondern um einen Vermerk zur Arbeitsperspektive der Beschwerdeführerin. Die aktuelle Arbeitssituation rechtfertigte nicht deren Einsicht in den Ordner „Referatsangelegenheiten“. Gleichwohl war es Unbefugten (dazu gehörte auch die Beschwerdeführerin) möglich, den Vermerk bei Abwesenheit des Gruppenleiters nach Beschaffung eines Zimmerschlüssels zu lesen. Dies wurde inzwischen verändert.

Die Abmahnung wurde in einem anderen Zusammenhang zurückgezogen.

Terminplaner als unzulässiger Datenträger ?

Im Vorzimmer der Amtsleiterin einer Behörde hing ein Terminplaner, auf dem namentlich die Abwesenheit aller im Amt beschäftigten Kollegen für das jeweils laufende Jahr für jeden Besucher ersichtlich war. Aufgrund der farblich unterschiedlichen Eintragungen konnte nachvollzogen werden, ob jemand wegen Urlaub oder Krankheit fehlte bzw. gefehlt hatte.

Da es sich bei Daten über krankheitsbedingte Fehlzeiten von Beschäftigten um höchst sensible Informationen handelt, die lediglich der personalaktenführenden Stelle oder der jeweiligen Einsatzstelle bekannt sein dürfen und von dieser vertraulich zu behandeln sind, ist diese Form der Anbringung von Terminplanern rechtswidrig. Diese sind nicht in Vorzimmern, wo sich häufig amtsfremde Personen aufhalten, sondern an einem anderen, geeigneten Ort aufzuhängen. Eine denkbare Alternative wäre auch eine Abdeckung.

Die Auffassung des Berliner Datenschutzbeauftragten wird geteilt.

Verwaltungsreform hinter dem Rücken der Mitarbeiter

Der Polizeipräsident beauftragte ein privates Projektbüro mit der Begleitung der Polizeistrukturreform Berlin. Zu diesem Zwecke wurden dem Büro Personaldaten (Name, Vorname, Dienstgrad und Dienststelle) von ca. 2000 Polizeibeamten übermittelt. Die Betroffenen wurden über diese Tatsache weder informiert noch um Zustimmung gebeten. Ferner sollten die betroffenen Beamten für einen Zeitraum von vier Wochen Erhebungsbögen führen, die ihre gesamten dienstlichen Tätigkeiten erfassen. Jedem Teilnehmer wurde durch das Projektbüro neben dem Erfassungsbogen ein sogenannter Identitätsbogen zugesandt, der eine Deanonymisierung zuließ.

Nach § 56 d Abs. 2 LBG dürfen Auskünfte an Dritte nur mit Einwilligung des Beamten erteilt werden, es sei denn, daß die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. Dies ist hier jedoch nicht der Fall. Zur Erfüllung der von dem Projektbüro vertraglich zugesicherten Aufgaben bzw. zur Durchführung der *externen Organisationsuntersuchung* hätte ein anonymisierter Datensatz ausgereicht. Bei der Fragebogenaktion hätten Name und Nummer in der Personalabteilung geführt werden können, um in Einzel-/Ausnahmefällen, z.B. bei unvollständigen Angaben oder fehlender Plausibilität, eine Klärung herbeiführen zu können.

Der Senat weist den in der Überschrift genannten Vorwurf, er habe die „Verwaltungsreform hinter dem Rücken der Mitarbeiter“ durchgeführt, zurück. Das gesamte Reformprojekt ist von der zuständigen Senatsverwaltung und der Polizeibehörde unter ständiger Beteiligung des Gesamtpersonalrates und auch der betroffenen Mitarbeiter vorbereitet und durchgeführt worden.

Die inhaltlichen Ausführungen des Berliner Datenschutzbeauftragten sind jedoch zutreffend. Die zuständige Senatsverwaltung und die Polizeibehörde waren dem Irrtum unterlegen, daß die Weitergabe der Personaldaten an das mit der Fortführung und Begleitung der Polizeistrukturreform beauftragte Consulting-Unternehmen nicht als Übermittlung anzusehen sind, sondern im Rahmen der Auftragsdatenverarbeitung weiter-

Der Personalrat einer Außenstelle des Landesschulamts beschwerte sich über einen Schulaufsichtsbeamten, der von den Schulleitern die Führung einer Liste verlangte, in der der Grund der Abwesenheit von Lehrkräften detailliert erfaßt werden sollte.

Der Schulaufsichtsbeamte begründete sein Vorgehen damit, solche Aufzeichnungen seien notwendig für die tägliche Erstellung von *Vertretungsplänen* und als Nachweis für die Erfüllung des gesetzlichen Auftrages, den Unterrichtsausfall auf ein Minimum zu beschränken. Teil der Schulaufsicht sei auch die Fachaufsicht über die Schulen und die Dienstkräfte und dies schließe das Informationsrecht über alle dienstlichen Angelegenheiten ein. Ferner sei die Übersendung der Listen notwendig für tarif- und beamtenrechtlichen Entscheidungen sowie für Freistellungen für Fortbildungen.

Zugang zu Personaldaten dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. (§ 56 Abs. 3 LBG).

Aus der allgemeinen Dienstaufsicht durch die Schulaufsicht kann kein umfassendes Vorlagerecht aller dienstlich relevanten Daten von Lehrern gefolgert werden. Denn für die Erstellung z.B. von Vertretungsplänen oder anderen organisatorischen Maßnahmen ist die Schulleitung vor Ort und nicht die Schulaufsicht zuständig. Die übrigen von dem Schulaufsichtsbeamten aufgeführten Beispiele betrafen vornehmlich den Zuständigkeitsbereich der personalaktenführenden Stelle und berührten nur in Ausnahmefällen die Zuständigkeit der Schulaufsicht.

gegeben werden dürfen.

Personaldaten zur „Auflockerung"?

Ein Bewerber für den mittleren Dienst bei der Berliner Schutzpolizei wandte sich mit folgendem Sachverhalt an uns: Anläßlich eines Einstellungstests wurden von einem Mitglied der Personalkommission im Beisein sämtlicher Mitbewerber die im Vorfeld erhobenen Personaldaten zum Teil sehr detailliert hinterfragt. Zwar konnte der jeweils Befragte danach den Raum verlassen, so daß sich die Zahl der „Mithörer" stetig reduzierte, jedoch konnte somit der letzte in der Bewerberrunde den beruflichen Werdegang der übrigen Mitbewerber erfahren.

Das Landespolizeiverwaltungsamt bestätigte diesen Vortrag und begründete die Vorgehensweise mit dem Bemühen der *Prüfungskommission*, möglichst jedem Bewerber vor den eigentlichen Prüfungsfragen die Prüfungsangst zu nehmen. So würden vor Beginn der Prüfung die einzelnen Kommissionsmitglieder vorgestellt und der Prüfungsablauf erläutert. Anschließend werde jedem Bewerber die Möglichkeit gegeben, sich der Kommission und den anderen Prüfungsteilnehmern persönlich vorzustellen. Diese Vorstellung sei freiwillig und habe keinen Einfluß auf das Prüfungsergebnis, beschränke sich auf Angaben über Namen, Schulzeit, ggf. den beruflichen Werdegang und etwaige Hobbys des Bewerbers. Ferner werde den Bewerbern stets mitgeteilt, daß die Beantwortung von Fragen zu ihrem Lebenslauf freigestellt sei und sie darauf nicht antworten müßten.

Es kann dahingestellt bleiben, ob die persönliche Vorstellung der Prüflinge vor der Auswahlkommission zur Auflockerung und Verbesserung der Prüfungsatmosphäre führt, da die Prüflinge jedenfalls nicht zu einer Offenlegung ihres beruflichen Werdegangs und privaten Hobbys vor den übrigen Prüflingen

Die Auffassung des Berliner Datenschutzbeauftragten wird nicht geteilt; ungeachtet dessen werden bei der Eignungsfeststellung für den mittleren Dienst der Schutzpolizei persönliche Daten der genannten Art im Beisein von Mitbewerbern nicht mehr erfragt.

gezwungen werden dürfen. Der Hinweis auf die Freiwilligkeit dieser Angaben ändert daran nichts, da kein Prüfling vor einer über seine berufliche Zukunft entscheidenden Auswahlkommission auf seinem Recht auf Selbstbestimmung bestehen wird. Selbstbestimmung setzt Entscheidungsfreiheit voraus. Der Betroffene muß, ohne einen Nachteil befürchten zu müssen, die Einwilligung auch verweigern dürfen.

Wir haben empfohlen, das Verfahren zu ändern und künftig die angestrebte Prüfungsatmosphäre im Rahmen von Einzelgesprächen herzustellen.

Akteneinsicht

Vom Personalamt einer Senatsverwaltung erhielten wir den Hinweis, es bestehe Unklarheit darüber, in welchem Verhältnis das Informationsrecht der Schwerbehindertenvertretung einerseits und die datenschutzrechtlich gebotene vertrauliche Behandlung schutzwürdiger Personaldaten andererseits zueinander stehen.

Aufgabe der Schwerbehindertenvertretung ist es, die Eingliederung der Schwerbehinderten zu fördern, die Interessen der Schwerbehinderten zu vertreten und ihnen helfend und beratend zur Seite zu stehen. Das Schwerbehindertengesetz stattet die *Schwerbehindertenvertretung* zur Erfüllung ihrer Aufgaben gegenüber dem Arbeitgeber mit einem umfassenden Informationsrecht aus (§ 25 Abs. 2 Schwerbehindertengesetz – SchwBG –). Die Schwerbehindertenvertretung ist vom Arbeitgeber in allen Angelegenheiten, die einen Schwerbehinderten oder die Schwerbehinderten als Gruppe berühren, rechtzeitig und umfassend zu unterrichten und vor einer Entscheidung zu hören.

Zwar ist nach § 26 Abs. 6 SchwBG die Schwerbehindertenvertretung verpflichtet, über die ihr bekanntwerdenden persönlichen Verhältnisse und Angelegenheiten von Beschäftigten Stillschweigen zu bewahren. Gleichwohl kann nicht ohne weiteres davon ausgegangen werden, schwerbehinderte Dienstkräfte sind stets damit einverstanden, daß die Schwerbehindertenvertretung auch Informationen über Angelegenheiten erhält, die höchst private Sachverhalte einschließen können.

Aus dem Kontext des Gesetzes, insbesondere aus dem ersten Satz des ersten Absatzes des § 25 SchwerBG, aber auch aus dem Sinn und Zweck der Vorschrift folgt, daß bei der Formulierung „in allen Angelegenheiten" nur die Umstände gemeint sind und gemeint sein können, die den Schwerbehinderten entweder bezüglich seines Dienst- bzw. Arbeitsverhältnisses oder seine Behinderung betreffen. So haben beispielsweise der Antrag auf Gewährung eines Vorschusses, die Gewährung von Sonderurlaub unter Fortfall der Vergütung oder die Gewährung oder der Wegfall von kinderbezogenen Anteilen im Ortszuschlag keinen ursächlichen Bezug zur Arbeit, lassen hingegen Rückschlüsse auf die finanzielle Situation des Schwerbehinderten bzw. dessen Kindes zu und gewähren unnötigerweise Einblicke in dessen Privatsphäre. Eine Beteiligung der Schwerbehindertenvertretung wäre daher nicht erforderlich und datenschutzrechtlich unzulässig.

Die Auffassung des Berliner Datenschutzbeauftragten wird geteilt.

Auskunft an Betroffenen

In der Senatsverwaltung für Justiz war es bislang unüblich, Teilnehmern an Eignungsprüfungen, die u.a. ein Diktat sowie einen Intelligenzstrukturtest beinhalten, die erreichte Punktzahl und Fehler in der Rechtschreibung mitzuteilen bzw. zu erläutern.

Die Vorgehensweise der Senatsverwaltung ist mit dem Recht

Der seitens der Berliner Datenschutzbeauftragten

des Betroffenen auf Auskunftserteilung nach § 16 BlnDSG nicht zu vereinbaren. Danach hat jeder nach Maßgabe dieses Gesetzes ein Recht auf Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten. Sind personenbezogene Daten in Akten gespeichert, so kann der Betroffene bei der datenverarbeitenden Stelle *Einsicht in die Akten* verlangen (§ 16 Abs. 4 BlnDSG).

Zukünftig werden den Bewerbern auf Wunsch die jeweiligen Einzelergebnisse mitgeteilt sowie die Testunterlagen zur Einsichtnahme zur Verfügung gestellt.

Integriertes Personalverwaltungsverfahren – IPV

Die Personalverwaltung des Landes soll in Zukunft mit einem modernen IT-Verfahren, dem Integrierten Personalverwaltungsverfahren – IPV – durchgeführt werden. Die Planung und Entwicklung ist derzeit so weit fortgeschritten, daß in einem Bezirksamt (Köpenick) die Pilotanwendung begonnen hat.

Das Projekt IPV ist sowohl ein Organisationsprojekt als auch ein IuK-Projekt. Es bewirkt organisatorische Veränderungen im Personalwesen, die auch im Einklang mit den Zielen der Verwaltungsreform stehen. Sie führen zur Straffung von Abläufen, die durch IPV unterstützt werden und gehen einher mit notwendigen Regeländerungen, so vor allem die Zahlungsbestimmungen für die Bezügeverfahren.

IPV betrifft die dezentralen Bereiche des Personalwesens: Stellenbewirtschaftung, Personalaktenführung, Lohn- und Gehaltsstelle. Die Zahlungsverfahren (Personalbezügeverfahren) werden nach wie vor mit den bisherigen Systemen des Landesamtes für Informationstechnik (LIT) im Auftrag des Landesverwaltungsamtes (LVwA) durchgeführt. Da IPV für viele Bereiche eine Erstautomation darstellt, müssen Schnittstellen zwischen IPV und Personalbezügeverfahren im IPV-Projekt geplant werden.

Mit IPV werden die *dezentralen Bereiche des Personalwesens* mit lokalen Client-Server-Netzen mit UNIX-Servern und PC-Arbeitsplätzen ausgestattet. Diese lokalen Netze sollen über das MAN die Dienste des Service- und Administrationszentrums im LIT in Anspruch nehmen, sobald die dafür erforderlichen Sicherheitsfunktionen (Verschlüsselung) bereitstehen. Ferner sind zentrale Betreuungsinstitutionen vorgesehen, die ebenfalls über das MAN angeschlossen werden, jedoch auf keine personenbezogenen Daten zugreifen sollen. Der Datenaustausch mit den Personalbezügeverfahren erfolgt zunächst mit Datenträgern, später unter der Nutzung des MAN über Filetransfer.

Die Zusammenlegung von Funktionsbereichen ist datenschutzrechtlich relevant. So werden die personalaktenführenden Stellen und die Gehalts- und Lohnstellen zum „Personalservice" zusammengeführt. Dies bedeutet, daß weniger Personen mit den Personaldaten in einem Geschäftsvorfall in Berührung kommen müssen, diese benötigen jedoch mehr Daten für die Geschäftsvorfälle als zuvor.

Unsere wichtigsten ergänzenden Empfehlungen betrafen

– den *Zugang auf die Datenbank-Schnittstelle:* Er muß dem normalen Anwender durch wirksame Maßnahmen der Zugriffskontrolle verwehrt sein, denn seine Auswertungen haben sich auf die vorgesehenen und rechtlich geprüften Auswertungen zu beschränken. Die Datenbank-Schnittstelle darf nur im Ausnahmefall für nicht von vornherein planbare, aber im Einzelfall erforderliche Auswertungen genutzt werden. Die Nutzung sollte revisionssicher dokumentiert werden, möglichst auch automatisch zu protokolliert. Um den Anforderungen der

beanstandete Mangel wurde zwischenzeitlich behoben: Teilnehmern an Eignungsprüfungen für den allgemeinen Justizvollzugsdienst, die u.a. ein Diktat sowie einen Intelligenzstrukturtest beinhalten, werden auf Anfrage die erreichte Punktzahl sowie Fehler in der Rechtschreibung mitgeteilt bzw. erläutert.

Der Zugang zur Datenbank-Schnittstelle ist normalen IPV-Anwendern durch die gemäß Berechtigungskonzept aktivierten Berechtigungsmechanismen systemtechnisch verwehrt. Welche Auswertungen (Reports) vorgenommen werden dürfen, ist eindeutig in einem den geltenden Rechtsvorschriften entsprechenden Reportkatalog festgelegt, der mit dem Hauptpersonalrat (HPR) abgestimmt und bedarfsentsprechend fortgeschrieben wird. Darüber hinaus gehende Auswertungen gestattet das System den Anwendern nicht. Nutzungen der Datenbank-Schnitt-

Rahmen-Dienstvereinbarung über die Personal-Datenverarbeitung zu genügen, sollte dabei die Beteiligung des Personalrats in Dienstvereinbarungen vorgesehen werden;

– die spätere *Nutzung des MAN* für die Datenkommunikation: Sie darf erst erfolgen, wenn die vorgesehene Sicherheitsfunktionen des MAN zur Verfügung stehen oder wenn eine detaillierte Risikoanalyse die Unangreifbarkeit der Server gegen unbefugte Zugriffe von außen erwiesen hat. Dies gilt auch für die Datenübertragung für die Datensicherung im Sicherheitsrechenzentrum des LIT;

– den datenschutzgerechten Einsatz des *Client-Server-Systems:* Es ist durch das Client-Server-System sicherzustellen, daß sensible personenbezogene Daten nicht auf ungeschützten Bereichen der Clients abgelegt werden können;

– die Verantwortungsverteilung im sog. *Betreiberkonzept:* Die Verantwortungsverteilung zwischen Betreibern und datenschutzrechtlich verantwortlichen Stellen ist datenschutzrechtlich korrekt zu regeln. Betreiber dürfen keine Rechte erhalten, die der Verantwortung der datenverarbeitenden Stelle zuwiderlaufen.

stelle werden automatisch protokolliert. Aufgezeichnet wird, wer wann welche Auswertungen mit welchen Parametern durchgeführt hat.

In Köpenick erfolgt noch keine Datenkommunikation über das BeLa (früher MAN). Eine Nutzung des BeLa zur Übertragung von Personaldaten ist erst bei Bezirken/Senatsverwaltung mit personaldatenverarbeitenden Außenstellen erforderlich. Eine derartige Nutzung des BeLa wird nur in Verbindung mit einem Datenverschlüsselungssystem und nach einem Wirksamkeitsnachweis erforderlicher Sicherheitsmechanismen erfolgen.

Es ist grundsätzlich vorgesehen, Datensicherungen im Sicherheitszentrum des Landesamtes für Informationstechnik durchführen zu lassen. Zur Zeit werden die Daten allerdings bei der IPV-nutzenden Stelle gesichert.

Bei Clients unter Windows NT wird gewährleistet, daß keine Daten auf ungeschützten, d.h. nicht durch Paßwort gesicherten Bereichen des Clients, abgelegt werden können. Die Projektgruppe IPV empfiehlt daher den IPV-einsetzenden Verwaltungsbereichen den Einsatz von Windows NT.

Durch die Rollenbestimmung im Betreiberkonzept und das Berechtigungskonzept sind die Zuständigkeiten und Verantwortlichkeiten so zwischen den Betreibern von IPV und datenschutzrechtlich verantwortlichen Stellen aufgeteilt, daß keine Bestimmung zum Datenschutz verletzt wird.

Das IPV-Verfahrenssicherheitskonzept (Bestandteil des Betreiberkonzepts) entspricht den Anforderungen, die sich für den Einsatz von IT-Verfahren wie IPV aus dem IT-Sicherheitsrahmenkonzept ergeben.

4.4.2 Datenverarbeitung in der Medizin

Patientendaten im Internet?

Eine ärztliche Berufsorganisation fragte an, ob und in welcher Form das Internet im ärztlichen Bereich genutzt werden könnte.

Das Internet könnte sowohl als *Übertragungsmedium* für Patientendaten wie auch als bloßes *Recherchemedium* genutzt werden.

Es mag für manchen Arzt verlockend erscheinen, die Krankengeschichte, zu der er einen Kollegen telefonisch um Rat fragen möchte und die sowieso auf dem Computer vorhanden ist, diesem Kollegen auch gleich über das einfach zu erreichende Medium Internet direkt auf dessen Computer zu übertragen, damit der Kollege alle Daten selber auf dem Bildschirm verfügbar hat.

Wegen der potentiellen Unsicherheit des Internet dürfen aber Patientendaten, die ausnahmslos dem verschärften Schutz der ärztlichen Schweigepflicht unterliegen, stets *nur in zuverlässig verschlüsselter Form* mit elektronischer Post (E-Mail) über das Internet geschickt werden. Die bloße Absicherung eines Krankenhaus- oder Praxisnetzes gegen einen „Angriff" von außen durch Firewalls reicht nicht aus, da die elektronische Post den geschützten Bereich in jedem Fall verläßt. Eine globale Veröffentlichung von Patientendaten – nichts anderes wäre eine unverschlüsselte Versendung im Internet – hätte auch strafrechtliche Konsequenzen für den Absender.

Da die elektronische Post sich gegenwärtig ebenso durchzusetzen beginnt wie zuvor die Faxkommunikation und zu einem unbewußt und unkritisch genutzten Medium entwickelt, ist eine rasche Aufklärung des ärztlichen Benutzerpersonals über die

Risiken dringend notwendig.

Wegen des technisch kaum zu beherrschenden Risikopotentials des Internet (ein Einsatz von gestaffelten Firewalls ist teuer und kompliziert) auch im Hinblick auf die Einschleppung von Computerviren durch unbedacht agierende Internetnutzer (insbesondere Makro-Viren in Dokumenten), ist außerdem jede Zugangsmöglichkeit zum Internet auf einzelne *dedizierte* (d.h. vom restlichen Krankenhaus- oder Praxisnetz getrennte) PCs zu beschränken. Auch für Zwecke der bloßen Recherche im Internet darf kein Rechner verwendet werden, auf dem patientenbezogene Informationen gespeichert sind oder von dem aus auf solche Informationen zugegriffen werden kann.

Neben den datenschutzrechtlichen Fragestellungen darf im Hinblick auf mögliche „Viren-Verseuchungen" auch die Frage einer möglichen Haftung eines Benutzers der Internetdienste (und evtl. des Netzwerkverantwortlichen) nicht unberücksichtigt gelassen werden, denn ein „Virus" könnte auch Patientendaten innerhalb einer Datenbank unbemerkt durcheinanderbringen. Die Folgen können für die betroffenen Patienten buchstäblich tödlich sein.

Von einer medizinischen Fakultät wurde angefragt, ob die in der studentischen Ausbildung verwendete Krankheitsgeschichte („Paper-cases") im Internet der interessierten Öffentlichkeit zur Verfügung gestellt werden könnten. Die hierbei verwendeten Krankheitsgeschichten stimmen bis auf den geänderten Namen in allen medizinisch relevanten Daten mit dem realen Fall überein.

Da es sich bei einer Veröffentlichung im Internet nicht mehr um eine Verwendung der Krankheitsgeschichten zum Zwecke der medizinischen Behandlung handelt, liegt in der Veröffentlichung eine Zweckänderung der Daten. Zwar sehen sowohl das BDSG (§ 14 Abs. 3 S. 2) wie auch das BlnDSG (§ 11 Abs. 4 S. 3) und das Landeskrankenhausgesetz von Berlin (§ 26) eine Verarbeitung oder Nutzung von Patientendaten zu Ausbildungszwecken vor, jedoch dürfen dieser keine schutzwürdigen Interessen der Betroffenen entgegenstehen.

Nach Vorstellung der medizinischen Fakultät sollten zwar die Krankheitsgeschichten durch bloßes Verändern des Patientennamens anonymisiert werden. Eine *hinreichende Anonymisierung* setzt jedoch voraus, daß ein Patient nicht durch die Verwendung seiner Daten reidentifiziert werden kann. Eines der zur Veröffentlichung im Internet vorgesehene „Paper-cases" enthielt folgende Daten: Alter, Geschlecht, Beruf, Arbeitgeber nebst Arbeitserkrankung, Einlieferungszeit, Name der Klinik und Vorerkrankung nebst Diagnose durch die Hausärztin. Mit diesen Angaben könnte der Patient leicht herausgefunden werden. Eine bloße Namensänderung reicht für eine Anonymisierung nicht aus.

Auf der anderen Seite ist es fraglich, ob überhaupt eine vollständige Anonymisierung der Krankheitsgeschichte ohne Verfälschung des Ausbildungsmaterials möglich ist. Daraus folgt, daß die *„Paper-cases"* nur für die interne Ausbildung der medizinischen Fakultät Verwendung finden können und für eine globale Verbreitung nicht geeignet sind. Helfen könnte nur eine Einwilligung in die Veröffentlichung per Internet. Aber eine solche Einwilligung würde aus einer Zwangssituation heraus erfolgen, da der Patient vor seiner Behandlung bei Verweigerung der Einwilligung um den Erfolg derselbigen fürchten und nach erfolgter guten Behandlung sich in einer Phase der Dankbarkeit zu dieser Einwilligung genötigt sehen könnte.

Daher steht eine Veröffentlichung von medizinischen „Paper-cases" im Internet auch auf Grund einer Einwilligung im Wider-

Personenbezogene Daten dürfen grundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben oder gespeichert worden sind. Die Veröffentlichung einer Krankheitsgeschichte im Internet allein zur Information einer interessierten Öffentlichkeit erfüllt diese Voraussetzungen nicht, vielmehr ist in einer derartigen generellen Veröffentlichung eine Verarbeitung zu anderen Zwecken zu sehen.

Die Voraussetzung, unter der eine Übermittlung zu Aus- und Fortbildungszwecken oder Forschungszwecken zulässig wäre, müßte im Einzelfall geprüft bzw. als gegeben festgestellt werden (§ 14 Abs. 2 Nr. 9 und Abs. 3 S. 2 BDSG; § 11 Abs. 4 S. 3 BlnDSG; § 26 Abs. 2 S. 2 und Abs. 4 LKG).

spruch zur ärztlichen Berufsordnung.

„Die virtuelle zerebrale hirnorganische Ausfallerscheinung"

Eine geistig sehr frische Persönlichkeit, in Berlin lebend und mit vielen anderen Berlinern das Schicksal eines gleichlautenden Vor- und Nachnamens teilend, erhielt im Sommer 1994 die Rechnung einer Berliner Krankenkasse über einen 3-tägigen stationären Aufenthalt in den Karl-Bonhöffer-Heilstätten vom Februar 1994.

Da diese Person jedoch niemals dort behandelt wurde, ließ sie die Angelegenheit mit der AOK Berlin telefonisch klären. Der Irrtum wurde durch die Krankenkasse (telefonisch) bestätigt. Im September 1995 wurde diese Person wegen eines versicherungsrechtlichen Anspruchs von einem Arzt des *Medizinischen Dienstes* aufgesucht, der ihr aus seinen mitgeführten Akten folgende Diagnose verlas: „... zerebrale hirnorganische Veränderungen ... – ... Ausfallerscheinungen, usw. usw."! Dem Einwand, daß es sich dabei um eine bereits richtiggestellte Verwechslung handle, nahm der Arzt zur Kenntnis, beharrte bei den nachfolgenden Untersuchungen jedoch auf der bestehenden Aktenlage und stellte dieser geistig völlig gesunden Persönlichkeit folgende Fragen: „Wieviel ist Hundert weniger Sieben – ... In welcher Jahreszeit ist es am wärmsten? ... usw. usw."

Zwei weitere Beschwerden blieben ohne jede Reaktion. Erst als der Hausarzt sich an die AOK wandte, erhielt dieser im November 1995 den Anruf eines Mitarbeiters der AOK, der wörtlich sagte: „...da hat sich wohl irgend jemand einen schlechten Scherz mit ihnen erlaubt – die Sache ist erledigt!". Nachdem noch immer keine schriftliche Bestätigung über das Löschen dieser Daten erfolgt war, wurde auf eine erneute telefonische Rückfrage einer Vertreterin der Versicherten durch Mitarbeiter der AOK erklärt, „... daß sie als zuständige Sachbearbeiterin keinen Anlaß sehe, etwas aufgrund der Einwände zu ändern oder zu reagieren", denn „...wenn jemand als hilflose Person irgendwo in Wedding aufgelesen werde, kann diese sich auch nicht mehr daran erinnern" ..., „demzufolge bestehe auch kein Handlungsbedarf bei Einwänden und auch kein Bedarf zu reagieren oder diese ernstzunehmen."

Dieser Vorfall, bei dem die *Stigmatisierung nach Aktenlage* selbst bei einem ärztlich ausgebildeten Mitarbeiter des Medizinischen Dienstes stärker wirkte als der untersuchte Patient der vor ihm stand, ist besonders beklemmend. Fast zwei Jahre hat es gedauert, bis diese falsche Information aus den Akten entfernt wurde. Ursache war in der Tat eine Gleichheit von Namen und Vornamen, wobei das unterschiedliche Geburtsdatum von den Mitarbeitern der AOK übersehen worden war. Die AOK hat versichert, daß derartige Namensverwechslungen durch Sicherungsmaßnahmen im EDV-Programm für die Zukunft ausgeschlossen worden seien. Fehlspeicherungen zu falschen Personen seien somit nicht mehr möglich.

Der Senat bedauert diesen Vorfall. Die AOK Berlin wurde um eine Stellungnahme zum Sachverhalt, insbesondere zur unverhältnismäßig langen Dauer der Bereinigung des Fehlers, sowie um eine Erläuterung der im einzelnen getroffenen Maßnahmen zur Verhinderung der Fehlspeicherung bei Namensverwechslungen gebeten. Der Senat wird diese dem Berliner Datenschutzbeauftragten bei Vorliegen zur Kenntnisnahme reichen.

Organisationsmängel bei der Datenverarbeitung

Auch bei der Organisation der Datenverarbeitung im Bereich Gesundheit gibt es Menschliches, ja allzu Menschliches zu berichten, wie die Entwendung eines Computers aus einem Berliner Krankenhaus, und zwar aus der Chirurgie mit allen dort gespeicherten Patientendaten, oder das Auffinden von Operationsberichten des Krankenhauses Neukölln auf einer Straße in Friedrichshain. Die Staatsanwaltschaft hat die Vorfälle nicht aufklären können, Jedenfalls liegt ein datenschutzrechtlicher Mangel bei der Organisation der Datenverarbeitung vor. Ein Krankenhaus ist verpflichtet, die Datenverarbeitung so zu organisieren, daß unabhängig von persönlichen Schuldfragen die

Der Senat teilt nicht die Auffassung des Berliner Datenschutzbeauftragten, daß den beiden geschilderten Fällen ein datenschutzrechtlicher Organisationsmangel zugrundegelegen hat. Hinsichtlich der Entwendung eines Computers aus einem Berliner Krankenhaus hat das Krankenhaus Anzeige erstattet. Da sich der fragliche Computer im gesicherten Bereich der Operationsabteilung des Krankenhauses befand und darüber hinaus der Zugang zu diesem Computer nur über – Außenstehenden unbekannte – Paßwörter möglich war, liegt ein Organisationsmangel des Krankenhauses nicht vor. Ein solcher Diebstahl ist letztlich

Ursache derartiger Mängel aufgeklärt werden kann.

Auch im Gesundheitswesen besteht weiterhin der Trend, Verwaltungsfunktionen auszulagern, wobei auch Patientendaten, die der ärztlichen Schweigepflicht unterliegen, betroffen sein können. Dies ist nicht in jedem Fall ausgeschlossen. Wir haben es gebilligt, daß ein Krankenhaus einen privaten Unternehmer mit der endgültigen Archivierung der Krankengeschichten beauftragt hat. Es war sichergestellt, daß der Fremdunternehmer inhaltlich keinen Zugriff auf Patientendaten nehmen kann, die jeweils in Containern transportiert und gelagert werden. Bei Bedarf kann das Krankenhaus die Akte zurückholen und in die Behandlung einbringen. Auch der Medizinische Dienst der Krankenkassen von Berlin hatte die Auslagerung des Schreibdienstes auf externe Schreibbüros erwogen. Hiervon haben wir jedoch abgeraten, da angesichts der Vielzahl einzelner Vorfälle mit erheblichen Transportrisiken zu rechnen ist. Stattdessen haben wir empfohlen, besser fremde Schreibkräfte bei Bedarfsspitzen in den Geschäftsbereich des Medizinischen Dienstes hereinzuholen und mit entsprechender Schweigeverpflichtung dort zeitweilig zum Abbau von Spitzenlasten einzusetzen.

nicht zu verhindern.

Die vorgenannte Sicherung kann insofern als grundsätzlich ausreichend gelten.

Das Auffinden von Operationsberichten des Krankenhauses Neukölln auf einer Straße in Friedrichshain ist entgegen der Annahme des Berliner Datenschutzbeauftragten aufgeklärt worden. In diesem Fall hatte ein im Krankenhaus vormals tätiger Gynäkologe die für seine Facharztweiterbildung erforderlichen Operationsberichte widerrechtlich mit nach Hause genommen, die er dann – ebenso widerrechtlich – mit anderem „Müll“ entsorgen ließ. Ein derartiges eigenmächtiges Handeln eines Arztes kann nicht als Organisationsmangel des Krankenhauses angesehen werden. Ein Krankenhaus kann nur durch regelmäßige Rundschreiben auf die Einhaltung des Datenschutzes hinweisen. Es läßt sich nicht vermeiden, daß sich im Einzelfall ein Mitarbeiter nicht danach verhält. Im übrigen verweist der Senat insofern auf den ausführlichen Schriftwechsel zwischen dem Berliner Datenschutzbeauftragten und der zuständigen Fachverwaltung.

Einkommensdaten in medizinischen Gutachten?

Ein Patient beschwerte sich darüber, daß in einer gutachterlichen Stellungnahme des Medizinischen Dienstes der Krankenkassen unter dem Unterabschnitt „Sozialanamnese” detaillierte Einkommensdaten und Vermögensangaben enthalten waren, die er zwar im Gutachtergespräch offenbart hatte, sich jedoch nicht eine Vorstellung davon gemacht hätte, daß diese Daten später sein Gutachten zieren würden.

Dies ist selbstverständlich nicht erforderlich. Der Medizinische Dienst reagierte sehr positiv auf unsere Kritik und holte nicht nur in diesem konkreten Fall das Gutachten, das zum Teil an andere Stellen bereits versandt worden war, wieder zurück, sondern er veränderte es auch so, daß konkrete Angaben herausgestrichen wurden und nur noch das Ergebnis der Sozialanamnese erhalten blieb. Darüber hinaus erklärte er sich bereit, auch für künftige Fälle Formulierungsvorgaben zu liefern, die die konkrete Angabe von finanziellen Verhältnissen in einem ärztlichen Gutachten entbehrlich machen.

Der Medizinische Dienst der Krankenkassen wurde unter Bezugnahme auf den Vorgang um Übersendung der zugesagten Formulierungsvorgaben für künftige Fälle gebeten. Die Fachverwaltung sagt zu, bei Vorliegen der Antwort eine Durchschrift an den Berliner Datenschutzbeauftragten zu übermitteln.

4.4.3 Sozialdaten

Im vergangenen Jahr war das Verfahren zur Vergabe von Sozialleistungen Gegenstand vielfältiger Diskussionen. Einige spektakuläre Fälle der betrügerischen Erschleichung von Sozialhilfe haben Forderungen nach einer schärferen Kontrolle bewirkt, die bis zur generellen erkennungsdienstlichen Behandlung von Antragstellern reichen[104]. Vor diesem Hintergrund ist verwunderlich, daß das Bundesministerium für Gesundheit bis heute die Rechtsverordnung nicht vorgelegt hat, die einen Datenabgleich zwischen verschiedenen Sozialämtern ermöglicht (§ 117 Abs. 2 Bundessozialhilfegesetz – BSHG –).

Das Abgeordnetenhaus von Berlin hat den Senat im November 1996 aufgefordert, „geeignete Maßnahmen gegen Leistungsmißbrauch zu ergreifen. Insbesondere ist für die Vernetzung der Sozialämter der Bezirke inklusive einer „Kopfstelle” zu sorgen.” Die Senatsverwaltung für Gesundheit und Soziales meint, die Vernetzung der bezirklichen Sozialämter und die Bildung einer Kopfstelle sei schon vor Erlaß einer Rechtsverordnung durch das

Die hier erwähnten „Forderungen nach einer generellen erkennungsdienstlichen Behandlung von Antragstellern“ sind dem Senat in dieser Form nicht bekannt. Nach vorliegenden Erkenntnissen beschränken sich derartige Bestrebungen auf den Personenkreis der Kriegs- und Bürgerkriegsflüchtlinge, da hier Betrugsmöglichkeiten bestehen, die in der Vergangenheit erwiesenermaßen auch genutzt worden sind.

Solchen Betrugsmöglichkeiten kann nur wirksam entgegengetreten werden, wenn Mehrfachidentitäten durch entsprechende erkennungsdienstliche Behandlung ausgeschlossen werden können. Zu der Rechtsverordnung zu § 117 Abs. 2 BSHG, von der bereits ein Entwurf des Bundesministeriums für Gesundheit vorliegt und zu der sich die Senatsverwaltung für Gesundheit und Soziales – entsprechend dem Auftrag des Abgeordnetenhauses – äußern wird, ist im übrigen anzumerken, daß diese nur bedingt mit den Ausführungen zur erkennungsdienstlichen Behandlung in Verbindung steht, da diese Vorschrift enumerativ die übermittlungsfähigen Daten aufzählt

[104] vgl. oben 1.1, 3.1

Bericht des Berliner Datenschutzbeauftragten	Stellungnahme des Senats

Bundesgesundheitsministerium zulässig. Diese Rechtsauffassung ist jedoch unzutreffend. Der Berliner Gesetzgeber hat im Jahre 1994 durch eine Änderung des Gesetzes zur Ausführung des Bundessozialhilfegesetzes ausdrücklich klargestellt, daß die Vorschrift des Bundessozialhilfegesetzes, die einen Datenabgleich zwischen verschiedenen Sozialhilfeträgern zuläßt, zusammen mit der dazu zu erlassenden Rechtsverordnung auch auf den Datenabgleich zwischen den bezirklichen Sozialämtern in Berlin anzuwenden ist (§ 3 Ausführungsgesetz zum BSHG). Wenn der Bundesgesetzgeber das zuständige Bundesministerium ermächtigt hat, das Nähere über das Verfahren für einen solchen Datenabgleich durch Rechtsverordnung mit Zustimmung des Bundesrates zu regeln, dann sollte Berlin schon im Interesse eines möglichst bundeseinheitlichen Verfahrens (auf das der Senat in anderen Bereichen immer großen Wert legt) hier keinen Alleingang unternehmen.

und in dieser Aufzählung der „elektronische Fingerabdruck“ nicht enthalten ist.

Die Rechtsauffassung des Senats, daß die Vernetzung der bezirklichen Sozialämter und die Bildung einer Kopfstelle schon vor Erlaß dieser Rechtsverordnung möglich ist, hat der Senat in seinem Bericht über Maßnahmen gegen Leistungsmißbrauch – Drs. 13/576 – beschlossen

Pauschale Einholung von Bankauskünften

Zu einer Änderung der generalklauselartigen Pauschaleinwilligung in Bankauskünfte, die im *Antragsbogen A für die Sozialhilfe* enthalten ist, zwingt eine wichtige Entscheidung des Hessischen Verwaltungsgerichtshofes[105]. Die Pauschalität der Erklärung erzeugt weder eine rechtliche Verbindlichkeit noch einen wirksamen Druck, wahrheitsgemäßige Angaben zu machen. Stattdessen muß der Bürger von Anfang an über die rechtlich geregelten und tatsächlich durchgeführten Kontrollen und Datenabgleiche informiert werden. „Ohne Vorliegen konkreter Anhaltspunkte ist das Verlangen, der Einholung von Bankauskünften zuzustimmen, eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers und somit nicht ”erforderlich” im Sinne von § 60 Abs. 1 Nr. 1 Sozialgesetzbuch Buch I (SGB I).” Ein pauschaler Allgemeinverdacht gegenüber den von einem Hilfesuchenden abgegebenen Erklärungen und Angaben sei nicht ausreichend, dem Hilfesuchenden eine besondere Beweisführung aufzugeben. Auch die Befugnis des Sozialhilfeträgers, im Rahmen des ihm nach § 20 SGB X eingeräumten Ermessens über das Ausmaß der Ermittlungen zu entscheiden, bedeutete nicht, daß die Behörde davon ausgehen darf, die von dem Hilfesuchenden abgegebene Erklärung über seine Einkommens- und Vermögensverhältnisse könne unwahr sein, um sich auf diese Weise in betrügerischer Absicht Sozialhilfe zu erschleichen. Der Umfang der Ermittlungspflicht sei nicht in das Belieben der Behörde gestellt.

Der Senatsverwaltung für Gesundheit und Soziales[106] hat zwar neue *Grundsätze für das Verfahren bei der Erteilung von Auskünften über Bankkonten von Sozialhilfeempfängern* verfügt, die einen wesentlichen Fortschritt gegenüber der bisherigen Praxis darstellen. Wir vermissen jedoch noch immer, daß die Antragsteller über die in Frage kommenden Kontrollen (z.B. nach §§ 21 Abs. IV SGB X, 71 SGB X, 117 BSHG) regelmäßig informiert werden. Ein solcher Hinweis sollte generell erfolgen, weil jeder Antragsteller wissen sollte, welchen Überwachungsmöglichkeiten er sich bei der Stellung eines Leistungsantrages aussetzt, und vor allem unter welcher Voraussetzung von diesen weitreichenden Befugnissen in seinem Fall Gebrauch gemacht werden kann.

Die zuständige Fachverwaltung wird eine Änderung der Antragsbögen für Sozialhilfe vornehmen. Der Senat wird sich jedoch – entsprechend dem Auftrag des Abgeordnetenhauses von Berlin, Drs. 13/576, geeignete Maßnahmen zur Bekämpfung des Sozialleistungsmißbrauchs zu ergreifen – für eine Erweiterung der rechtlichen Möglichkeiten bei der Einholung von Bankauskünften durch eine entsprechende Gesetzesänderung einsetzen.

Zusammenlegung der Sozialen Dienste

Im Rahmen der Verwaltungsreform wurden die ehemaligen Abteilungen für Soziales und Gesundheit wie auch die Abteilun-

Die vom Berliner Datenschutzbeauftragten dargelegten organisatorischen Strukturveränderungen in einzelnen Bezirken

[105] Beschluß vom 7. Februar 1995 (– 9 TG 3113/94 -
[106] Schreiben v. 18. Oktober 1996, GeschZ.: VII A 28

gen für Jugend, Sport und Gesundheit in zahlreichen Bezirken Berlins unterschiedlich zusammengelegt. Einige haben die Abteilung für Gesundheit mit der Abteilung für Sozialwesen vereinigt, andere haben die Abteilungen für Jugend mit der Abteilung für Gesundheit verbunden. Einige Bezirke haben die alte Organisationsform in ihrer wesentlichen Struktur erhalten; teilweise wird die Zusammenlegung als unzulässig qualifiziert.

Kennzeichnend für alle Strukturveränderungen war, daß die im Gesundheitsamt bisher tätigen Mitarbeiter aus der Zuständigkeit des Amtsarztes herausgenommen, in die Abteilungen für Soziales oder für Jugend eingegliedert und der Leitung des dortigen leitenden Fachbeamten unterstellt wurden. Dies hat dazu geführt, daß diese Mitarbeiter keinen Zugang mehr zu den vom Amtsarzt geführten ärztlichen Aufzeichnungen haben dürfen.

Die *Aufgaben des Amtsarztes* ergeben sich aus dem Gesundheitsdienstgesetz (GDG). Insbesondere ist die sozialmedizinische Betreuung aufgeführt, die vom Amtsarzt auch mit Sozialarbeitern als ärztliche Aufgabe zu leisten ist (§ 22 Abs. 6 GDG). Für die Qualifikation der Tätigkeitsbereiche kommt es auf die ärztlichen Zielsetzungen und nicht auf die fachliche Qualifikation die ihm zugeteilten Mitarbeiter an. Deshalb unterliegen auch die sozialmedizinischen Aufgaben uneingeschränkt der ärztlichen Schweigepflicht. Hier eingesetzte Sozialarbeiter können sich also auf ein Zeugnisverweigerungsrecht berufen (§§ 53 Abs. 1 Ziff. 3, 53 a StPO).

Demgegenüber ist die Verpflichtung der Sozialarbeiter selbst auf *Geheimhaltung ihnen anvertrauter Tatsachen* nur im Ausnahmefall des Drogenberaters gerichtsfest (§ 53 Abs. 1 Ziff. 3 b StPO). Damit sind vertrauliche Unterlagen der Sozialarbeiter nicht vor einer gerichtlichen Beschlagnahme sicher. Das Sozialgesetzbuch X enthält in den §§ 68, 72 und 73 weitgehende Offenbarungsbefugnisse, die für den ärztlichen Bereich nicht gelten.

Die beschriebene organisatorischen Umstrukturierung widerspricht dem vom Gesundheitsdienstgesetz unterstellten Organisationsmodell und führt dazu, daß das vom Gesetzgeber gewollte sozialmedizinische Konzept nicht mehr in seiner bisherigen Form verwirklicht werden kann. Von Ärzten und von Sozialarbeitern der Gesundheitsämter sind wir darauf hingewiesen worden, daß insbesondere der Schutz für die am meisten gefährdeten Mitglieder der Gesellschaft, nämlich Säuglinge und Kleinkinder, erheblich geschwächt wird, weil die bisherige enge Verzahnung von medizinischer und sozialer Beratung für krisenanfällige Sozialmilieus von besonderem Vorteil war.

Die Umstrukturierung der Gesundheitsämter erschwert die sozialmedizinisch erforderlichen Datenflüsse zwischen Ärzten und ihren ehemals als Sozialarbeiter tätigen Erfüllungsgehilfen erheblich. Es bedarf eines zusätzlichen, oft die Akzeptanz verhindernden Einwilligungsverfahrens.

Sozialamt stört den Hausfrieden

Eine Frau beschwerte sich bei uns: Sie hatte bei ihrem Sozialamt Hilfe wegen der Kosten für den vom Vermieter installierten Kabelanschluß beantragt, jedoch einen ablehnenden Bescheid erhalten. Sie legte ihrer Sachbearbeiterin dar, daß bei einer Nachbarin (die von dem gleichen Sozialamt betreut wurde) diese Kosten übernommen worden seien und bat um Gleichstellung. Dabei sprach sie ausdrücklich nur von „einer Nachbarin" ohne deren Namen zu nennen. Wenige Tage später wurde sie von ihrer Nachbarin angesprochen, die ihr wutentbrannt vorwarf, sie

sind nach Auffassung des Senats rechtlich nicht zu beanstanden. Um die vom Berliner Datenschutzbeauftragten beschriebenen Auswirkungen zu vermeiden, wird der Senat dafür Sorge tragen, daß durch Erarbeitung von Verwaltungsvorschriften und durch Gespräche mit den beteiligten Fachverwaltungen eine Sicherung der sozialmedizinischen Ziele des Gesundheitsdienstgesetzes erreicht wird. Der besonderen Stellung des Amtsarztes und seiner Verantwortlichkeit für den Gesundheitsdienst als Ganzes ist dabei entsprechend Rechnung zu tragen.

hätte sie bei der Sachbearbeiterin angeschwärzt und müsse deswegen nun die Kabelanschlußgebühr zurückzahlen. Die weitere Aussprache der Damen ergab, daß die Sachbearbeiterin im Sozialamt gesagt hatte: „Sie können sich bei Frau Müller bedanken, daß sie das Geld zurück bezahlen müssen".

Selbstverständlich war hier ein Mangel festzustellen, weil das Sozialgeheimnis (§ 35 SGB I i.V.m. § 67 ff. SGB X) nicht gestattet, daß der Leistungsträger Daten eines Hilfeempfängers an dessen Bekannte in der Annahme vermittelt, daß beide ohnehin alles voneinander wüßten. Das zunächst schwer gestörte Verhältnis zwischen den Nachbarinnen konnte nur mühsam wiederhergestellt werden.

Nach Auffassung des Senates handelt es sich bei dem geschilderten Sachverhalt um einen bedauerlichen Einzelfall. Ein solches Verhalten einer Mitarbeiterin des Sozialamtes wird vom Senat nicht gebilligt.

Kindertagesstätten – „null Bock" auf Rechtsnormen

Die Regelungen des *Kindertagesstättenbetreuungsgesetzes* und die Fragebögen zur Feststellung des Betreuungsbedarfs führten zu erheblicher öffentlicher Erregung. Wir hatten auf die datenschutzrechtlichen Mängel des Verfahrens hingewiesen, insbesondere hatten wir auf die fehlende Rechtsgrundlage aufmerksam gemacht und gefordert, die nach dem Gesetz vorgeschriebene Rechtsverordnung zu erlassen[107]. Trotz mehrfacher Mahnungen ist dies nicht geschehen. Eine allgemeine Dienstvorschrift, mit der sich die Bezirksämter zu Beginn des Berichtsjahres behelfen mußten, stellt keine ausreichende rechtliche Grundlage dar. Auch die gesetzliche Verpflichtung zur Regelung der Datenverarbeitung bei der Berechnung der Kostenbeteiligung der Eltern an der Betreuung ihrer Kinder in städtischen Kindertagesstätten und in Tagespflege mißachtet die Senatsverwaltung für Schule, Jugend und Sport mittlerweile im vierten Jahr beharrlich[108].

Der Senat hält die in der Überschrift dieses Abschnitts gewählte Ausdrucksweise nicht für sachgerecht.

Die notwendige Umstellung des gesamten Anmelde- und Planungsverfahren als Basis der Neuordnung der Personalausstattung und Kita-Finanzierung nach den Vorgaben des Gesetzes zur Förderung und Betreuung von Kindern in Tageseinrichtungen und Tagespflege (KitaG) vom 19. Oktober 1995 erforderte eine Fülle von Regelungen. Deren Erarbeitung stand unter großem Zeitdruck, einerseits durch die späte und kurzfristige Verabschiedung des Kindertagesbetreuungsgesetzes, andererseits durch die Änderung des § 24 SGB VIII hinsichtlich der Stichtagsregelung und der Härtefallregelung durch das Zweite Gesetz zur Änderung des Achten Buches Sozialgesetzbuch vom 15. Dezember 1995, also erst kurz vor Inkrafttreten des Rechtsanspruchs auf einen Kindergartenplatz am 1. Januar 1996.

Es war in der Kürze der Zeit nicht möglich, die nach § 21 KitaG vorgesehene Rechtsverordnung mit dem erforderlichen Beteiligungsverfahren zu entwickeln. Angesichts des Handlungsdrucks der Jugendämter hat sich die Senatsverwaltung für Schule, Jugend und Sport daher für eine pragmatische Vorgehensweise entschieden. Dazu gehörte es, vorrangig die Instrumente zu entwickeln, die für die Anmeldung selbst und den erforderlichen Platznachweisen zum nächsten Kita-Jahr erforderlich waren. Im Interesse eines einheitlichen Verwaltungshandelns wurde festgelegt, das Anmeldeverfahren für 1996 durch Verwaltungsvorschriften abzusichern.

Der Datenschutzbeauftragte des Landes Berlin, der zunächst Einwände geltend gemacht hatte, äußerte mit Schreiben vom 26. Februar 1996 seine grundsätzliche Zustimmung zu dem Entwurf.

Die entsprechenden Ausführungsvorschriften über das Anmeldeverfahren, die Planung und den Nachweis von Plätzen in Tageseinrichtungen und Tagespflege (AV-Kita-Verf) traten am 15. März 1996 in Kraft.

Die Rechtsverordnung nach § 21 KitaG wird gegenwärtig erarbeitet und im Rahmen des Beteiligungsverfahrens selbstverständlich auch dem Berliner Datenschutzbeauftragten zur Mitzeichnung zugeleitet werden.

Der Senat nimmt die Kritik zur ausstehenden Regelung der Datenverarbeitung im Rahmen der elterlichen Kostenbeteiligung für die Unterbringung von Kindern in städtischen Kindertagesstätten und in Tagespflege zur Kenntnis. Die im Vordergrund stehende Umsetzung des Rechtsanspruchs auf einen Platz in

[107] JB 1995, 5.6
[108] JB 1995, 5.6

einer Tageseinrichtung für drei- bis sechsjährige Kinder und Maßnahmen zur Haushaltskonsolidierung haben die bei der Senatsverwaltung für Schule, Jugend und Sport vorhandene Arbeitskapazität vollständig gebunden. Der notwendige Erlaß der Bestimmungen zur Datenverarbeitung wird mit dem anstehenden Regelungsbedarf des Kindertagesstätten- und Tagespflegebereiches verknüpft werden.

4.4.4 Bauen und Wohnen

Bekämpfung der Zweckentfremdung von Wohnraum

Hat ein Gewerbetreibender sein Gewerbe nach der *Gewerbeordnung* pflichtgemäß angezeigt, wurde dies regelmäßig von den Wirtschaftsämtern an die für die Bekämpfung der Zweckentfremdung von Wohnraum zuständige Stelle – in der Regel die Wohnungsämter in den Bezirken – gemeldet.

Diese regelmäßige Datenübermittlung war unzulässig. In § 2 a Abs. 2 Satz 2 Zweckentfremdungsbeseitigungsgesetz (ZwBesG) ist geregelt, daß eine Übermittlung von Daten aus den Anzeigen Gewerbetreibender nach der Gewerbeordnung nur zu Klärung eines Sachverhaltes zulässig ist. Damit ist klargestellt, daß eine Übermittlung der Daten aller Gewerbeanzeigen davon nicht abgedeckt ist. Die Übermittlung aller Gewerbeanzeigen ist für die Erfüllung der Aufgaben nach dem ZwBesG auch nicht erforderlich. Die Senatsverwaltung für Wirtschaft und Betriebe hat dies bestätigt[109] und die Wohnungsämter aus der Liste der regelmäßigen Datenempfänger gestrichen.

Auch der *Umfang der Daten*, die im Zusammenhang mit den ZwBesG erhoben und verarbeitet werden, war Gegenstand von Überprüfungen. Das Wohnungsamt darf die in § 2 a ZwBesG genannten Daten erheben, soweit dies zur Erfüllung der Aufgaben erforderlich ist. Der Datenkatalog ist abschließend. Er kann nicht durch eine Einwilligung der Betroffenen erweitert werden. Die Daten sind grundsätzlich bei dem Betroffenen selbst und mit dessen Kenntnis zu erheben (§ 18 Abs. 4 ASOG). Nur unter engen Voraussetzungen ist eine Erhebung der Daten bei Dritten zulässig. Anfragen zu Daten aus dem Melderegister sind vor diesem Hintergrund ausschließlich an das Landeseinwohneramt Berlin[110] und nicht an das Bezirkseinwohneramt zu richten. Das Wohnungsamt kann die personenbezogenen Daten speichern, soweit dies zur Erfüllung der Aufgabe, zweckfremd genutzten Wohnraum wieder dem Wohnungsmarkt zuzuführen, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Mit Erlaß eines entsprechenden Bescheides und Ablauf der Rechtsmittelfristen oder einer rechtskräftigen gerichtlichen Entscheidung ist der Einzelvorgang abgeschlossen. Eine weitere Speicherung der Daten bzw. Aufbewahrung der Unterlagen ist nur für eine zeitlich befristete Dokumentation des ordnungsbehördlichen Verwaltungsverfahrens zulässig. Zur Begrenzung der Aufbewahrungsfrist ist zwischen der Erforderlichkeit für Dokumentationszwecke (z.B. Amtshaftungsansprüche, Nachfragen der Betroffenen, Überprüfung des Verfahrens) und dem mit der weiteren Speicherung verbundenen Eingriff in das *informationelle Selbstbestimmungsrecht* der Betroffenen abzuwägen. Dazu erscheint – mit Ausnahme einer weiteren Speicherung unter haushaltsrechtlichen Aspekten – eine Aufbewahrungsfrist der abgeschlossenen Vorgänge von einem Jahr ausreichend.

Auf unsere Hinweise reagierte das betroffene Wohnungsamt

[109] Rundschreiben Nr. 3/1996 vom 6. März 1996 unter Punkt 2.
[110] § 25 i.V. m. § 1 Abs. 2 MeldeG

wie folgt:

„Die in Ihrem Schreiben (...) gestellten Forderungen, nur Daten zu erheben, die durch die derzeit noch gültige Regelung des § 2 a Zweckentfremdungs-Beseitigungsgesetz gedeckt sind bzw. für die der Verfahrensbeteiligte ausdrücklich schriftlich sein Einverständnis erklärt hat (Anm.: mithin unserer Forderung gesetzmäßig vorzugehen), können und werden wir nicht erfüllen."

„Eine Auskunftsbefugnis ausschließlich des LEA zur Übermittlung melderechtlicher Daten (Fußnote: so verbindlich in § 25 MeldeG i.V.m. § 1 Abs. 2 MeldeG geregelt) stellt sich (...) als völlig unakzeptabel (...) dar. (...) Wir werden uns (...) weiter an unser bezirkliches Einwohneramt wenden."

„Die Aufbewahrung sämtlicher Vorgänge ist für die Bearbeitung der zweckentfremdungsrechtlichen Verfahren von großer Bedeutung. (...) Eine Vernichtung – gleich welchen Umfangs – stellt eine Behinderung der Aufgabenerfüllung dar."

Angesichts der angespannten Lage in bestimmten Bereichen des Wohnungsmarktes ist der Bekämpfung von zweckfremd genutztem Wohnraum große Bedeutung beizumessen. Dies kann jedoch nicht rechtfertigen, daß bestehende Gesetze als hinderlich für die Aufgabenerfüllung umgangen werden.

Inzwischen liegt ein *Entwurf zur Änderung von § 2 a ZwBesG* vor. In dem Entwurf wird dem Grundsatz der Verhältnismäßigkeit, den die Ordnungsbehörden gemäß § 11 ASOG zu beachten haben, nicht ausreichend Rechnung getragen. Sowohl der von der Datenverarbeitung betroffene Personenkreis als auch der Katalog der personenbezogenen Daten werden – im Vergleich zur bestehenden Regelung des § 2 a Abs. 1 ZwBesG – unverhältnismäßig erweitert.

Die Datenverarbeitungsbefugnisse des Entwurfes berühren in erheblichem Umfang fast alle Lebensbereiche und sehen massive Eingriffe in das Recht der informationellen Selbstbestimmung der Betroffenen vor. Nach dem Entwurf dürfen zur Bekämpfung der Zweckentfremdung von Wohnraum künftig Daten zu den

– Lebensumständen (z.B. Daten des gesamten – evtl. früheren – Mietvertrages, einschließlich besonderer Vereinbarungen, Miethöhe, Kundendaten der BEWAG, GASAG),
– persönlichen und sozialen Beziehungen (z.B. Daten zu Ehegatten, Kindern, Lebensgefährten),
– Kommunikationsbeziehungen (z.B. Kundendaten der Post, Telekom),
– wirtschaftlichen Verhältnissen (z.B. Daten aus Gewerbeanzeigen, Handelsregister, Sozialamt)

der Betroffenen erhoben und gespeichert werden.

Die Daten lassen sich bei der für die Bekämpfung der Zweckentfremdung von Wohnraum zuständigen Stelle problemlos zu einem Persönlichkeitsbild verbinden bzw. zusammenführen. Derartig umfangreiche Datenverarbeitungsbefugnisse sind sonst nur Sicherheitsbehörden unter restriktiven Voraussetzungen zugewiesen. Für die Bekämpfung von zweckfremd genutztem Wohnraum ist eine derartig umfangreiche Datenverarbeitung unverhältnismäßig.

Der Senat äußert sein Befremden darüber, daß im Rahmen des Tätigkeitsberichts des Berliner Datenschutzbeauftragten bereits auf Entwürfe zu Änderungsgesetzen eingegangen wird, die sich zur Zeit noch im Abstimmungsverfahren – auch mit dem Berliner Datenschutzbeauftragten – befinden. Hier sollte zunächst auf Fachebene die erforderliche Diskussion geführt werden, bevor einseitig dem noch nicht vorliegenden Ergebnis vorgegriffen wird.

In diesem Zusammenhang ist insbesondere darauf hinzuweisen, daß die Einschätzung des Berliner Datenschutzbeauftragten hinsichtlich des erforderlichen Umfangs der Erfassung und Verarbeitung von Daten zur Erfüllung der Aufgaben nach dem Zweckentfremdungsbeseitigungsgesetz (ZwBesG) und der 2. Zweckentfremdungsverbotsverordnung (2. ZwVbVO) vom Senat *nicht* geteilt wird.

Ebenso bestehen aus fachlicher Sicht Einwände gegen die Einschätzung über die erforderlichen Aufbewahrungsfristen für abgeschlossene Vorgänge, die noch weiterer Abstimmungen bedürfen.

Die Ergänzung der datenschutzrechtlichen Bestimmungen des ZwBesG und der 2. ZwVbVO ist für die Durchsetzung des Zweckentfremdungsverbots zwingend erforderlich, um zum einen die Anforderungen des Berliner Datenschutzgesetzes zu erfüllen und um den bezirklichen Wohnungsämtern als fachlich zuständige Stellen die notwendigen Sachaufklärungen zu ermöglichen.

Wohngeldantrag, Formular zu ergänzenden Angaben über Lebensunterhalt

Eine Bürgerin beschwerte sich über den Umfang der Datenerhebung eines Wohnungsamtes im Verfahren zur Beantragung von Wohngeld. Mit dem Fragebogen „Ergänzende Erklärung zum Antrag auf Wohngeld" sollte die

Bericht des Berliner Datenschutzbeauftragten	Stellungnahme des Senats

Antragstellerin Angaben zu den Aufwendungen u.a. für die Ernährung (Frühstück, Mittag- und Abendessen, Genußmittel), die Neuanschaffung, Reinigung und Ausbesserung von Bekleidung und Wäsche, Putz- und Reinigungsmittel, Körperpflege, Kosmetik, Medizin, Unterhaltung, Kultur (Bücher, Zeitungen, Zeitschriften, Kino, Theater, Rundfunk, Fernsehen usw.), Versicherungsbeiträge machen.

Das Wohnungsamt begründete den umfangreichen Fragenkatalog damit, daß bei der Bewilligung von Wohngeld als Sozialleistung in Einzelfällen differenzierte Nachfragen zum Einkommen erforderlich sind. Das betrifft vor allem Wohngeldantragsteller, deren ermitteltes Einkommen – auch bei Berücksichtigung eines zu gewährenden Wohngeldes – noch unterhalb des sozialhilferechtlichen Bedarfes liegt. In diesen selten auftretenden Fällen sind die Angaben des Antragstellers besonders sorgfältig auf Glaubwürdigkeit und Vollständigkeit zu überprüfen. Dazu wird der genannte Vordruck verwendet. Er dient als Entscheidungsgrundlage dafür, mit welcher Einkommenshöhe die Wohngeldberechnung erfolgen kann (Regelsatz der Sozialhilfe, Schätzung o.ä.).

Die Rechtsauffassung des Wohnungsamtes ist grundsätzlich zutreffend. Zweifelhaft ist jedoch, ob die umfangreiche Datenerhebung mit dem Vordruck erforderlich ist. Einzelne Fragestellungen können zu Datengruppen bzw. Oberpunkten zusammengefaßt werden. Das Formular sollte zudem um die nach § 67 a Abs. 3 SGB X erforderlichen Hinweise (Erhebungszweck, Freiwilligkeit bzw. Rechtsvorschrift auf die die Erhebung gestützt wird, Folgen der Verweigerung von Angaben) ergänzt werden. Das Wohnungsamt ist unserer Empfehlung gefolgt, hat den Fragebogen entsprechend redaktionell überarbeitet und dabei die Hinweise nach § 67 a Abs. 3 SGB X mit einbezogen.

Die Durchführung des Wohngeldgesetzes (WoGG) und des Wohngeldsondergesetzes (WoGSoG) ist eine Bezirksaufgabe unter Fachaufsicht. Dabei regeln die vom Bundesministerium für Raumordnung, Bauwesen und Städtebau herausgegebenen Verwaltungsvorschriften zum WoGG und Durchführungsvorschriften zum WoGSoG, daß bei einem Einkommen eines Wohngeldantragstellers unter dem Sozialhilfesatz die Angaben besonders sorgfältig zu prüfen sind. Grundsätzlich werden alle Wohnungsämter dieser Vorgabe durch entsprechende zusätzliche Fragebögen gerecht. Bei dem betreffenden Formular handelt es sich jedoch um einen bezirkseigenen Vordruck.

Der Senat begrüßt, daß die jetzt verwandte Fassung des Vordrucks, die zwischen dem betroffenen Wohnungsamt und dem Berliner Datenschutzbeauftragten abgestimmt wurde, offensichtlich nunmehr keinen Anlaß zu weiteren Beanstandungen gibt.

Mieterinformation bei Beantragung einer Abgeschlossenheitsbescheinigung

Im Jahresbericht 1993[111] haben wir darauf hingewiesen, daß die Information von Mietern über die Antragstellung des Hauseigentümers auf eine sog. *Abgeschlossenheitsbescheinigung* durch die Wohnungsämter nur auf Grund einer Rechtsvorschrift bzw. der Einwilligung des Betroffenen zulässig ist. Eine derartige Rechtsvorschrift ist nicht vorhanden; von einer Einwilligung des Antragstellers auf Abgeschlossenheitsbescheinigung ist nur im Ausnahmefall auszugehen. Im Interesse einer mieterfreundlichen Regelung hatten wir deshalb gesetzgeberische Aktivitäten angeregt.

Ein entsprechendes Gesetz zur Sicherung der Information der Mieter bei der Umwandlung in Wohneigentum (Informationssicherungsgesetz)[112] wurde von der Fraktion Bündnis 90/Die Grünen in das Abgeordnetenhaus von Berlin eingebracht und mit der Mehrheit der Stimmen von CDU und SPD abgelehnt. Ausschlaggebend für die Ablehnung war die Auffassung, daß es dem Land Berlin an der Gesetzgebungskompetenz fehle. Der Bundesgesetzgeber habe – mit Schaffung des § 570 b BGB – von seiner Gesetzgebungskompetenz nach Artikel 72 Abs. 1 Grundgesetz Gebrauch gemacht. Für ergänzende Regelungen sei kein Raum. Diese Auffassung teilen wir nicht. Im Bürgerlichen Gesetzbuch ist lediglich die Informationspflicht des Vermieters gegenüber dem Mieter vorgesehen. Das bedeutet nicht, daß der Gesetzgeber Unterrichtungen durch öffentliche Stellen ausschließen wollte. Ungeachtet dessen sollte sich das Land Berlin nicht auf diesen formalen Standpunkt zurückziehen und – im Interesse der betroffenen Mieter sowie einer datenschutzgerechten Verfahrensweise – eine Regelung auf Bundes-

Der Senat stellt fest, daß die im Datenschutzbericht 1993 beanstandete Form der Information der Mieter durch die Bezirksämter nicht mehr stattfindet. Die Anforderungen des Datenschutzes sind damit erfüllt.

Der Senat ist weiterhin der Auffassung, daß § 570 b BGB eine ergänzende Regelung durch das Land Berlin nicht zuläßt. Ob eine bundesrechtliche Lösung möglich ist, bleibt abzuwarten. Auf die ausführlichen Stellungnahmen im Rahmen des Antrages der Fraktion Bündnis 90/Die Grünen über das Gesetz zur Sicherung der Information der Mieter bei Umwandlung ihrer Wohnung in Wohneigentum – Drs. 12/3575, 13/317 – wird verwiesen.

[111] 4.2
[112] Drs. 13/317

ebene anstreben.

Auskünfte aus dem Liegenschaftskataster über eine Vielzahl von Grundstücken

Ein Bezirksamt bat, datenschutzrechtlich zu prüfen, ob einer Immobilienfirma Auskunft aus dem Liegenschaftskataster – einschließlich der darin enthaltenen Eigentümerangaben – zu ca. 400 einzeln benannten Grundstücken im Bezirk gewährt werden kann.

Schriftliche Auskünfte und Auszüge aus dem Liegenschaftskataster dürfen nach § 17 Abs. 4 Vermessungsgesetz (VermG) grundsätzlich auch über eine Mehrzahl von einzeln bestimmten Liegenschaften erteilt werden, soweit der Auskunftsbegehrende ein *berechtigtes Interesse* an den Angaben *glaubhaft macht*. Auch wirtschaftliche Bedürfnisse können ein berechtigtes Interesse darstellen. Dabei sind folgende Erwägungen zu berücksichtigen:

Neben den Grundstücks- und Gebäudedaten erhält der Auskunftsbegehrende auch Angaben über Namen, Geburtsnamen und Geburtsdaten der Grundstückseigentümer, Erbbau- und Nutzungsberechtigten (§ 16 Abs. 1 VermG) aus dem Liegenschaftskataster. Dadurch wird nicht unerheblich in die Persönlichkeitsrechte – insbesondere bei Massenauskünften – einer Vielzahl von Betroffenen eingegriffen. Insofern sind an die Glaubhaftmachung des berechtigten Interesses im Rahmen von § 17 Abs. 4 VermG gesteigerte Anforderungen zu stellen.

Zunächst ist dem Auskunftsbegehrenden – in einem abgestuften Verfahren – nur Auskunft über die *Grundstücksdaten* zu gewähren. Erst nachdem er sein berechtigtes Interesse konkretisiert hat, ist die Auskunft auf die o.g. personenbezogenen Daten der Eigentümer, Erbbau- und Nutzungsberechtigten zu erweitern. Zur Konkretisierung hat der Antragsteller die Anzahl, Lage und Art (z.B. Einfamilienhaus) der Liegenschaften zu bezeichnen und sein berechtigtes Interesse durch weitere Angaben – differenziert nach den betroffenen einzelnen Liegenschaften – (z.B. durch bestehende Kundenaufträge und die Absicht, an alle Eigentümer herantreten zu wollen) glaubhaft darzulegen. Wird dem Antragsteller danach Auskunft über eine Vielzahl von Liegenschaften gewährt, ist er darauf hinzuweisen, daß die Daten im Rahmen der von ihm gemachten Angaben einer Zweckbindung (§ 28 BDSG) unterliegen.

Eine Massenauskunft ist in jedem Fall dann unzulässig, wenn zu befürchten ist, daß durch die Vielzahl der betroffenen Grundstücke innerhalb eines begrenzten Regionalbereiches die Gefahr besteht, daß – parallel zum öffentlichen Liegenschaftskataster – ein nicht-öffentliches Register entsteht. Ein derartiges nicht-öffentliches Register widerspricht dem Schutzinteresse der Allgemeinheit (§ 17 Abs. 5 VermG) und steht im Widerspruch zu § 17 Abs. 8 VermG, wonach die Angaben aus dem Liegenschaftskataster nur für den Aufbau und die Aktualisierung von Informationssystemen öffentlicher Stellen zur Verfügung gestellt werden dürfen.

Das hier dargelegte Ergebnis der datenschutzrechtlichen Prüfung zum Thema „Auskünfte aus dem Liegenschaftskataster über eine Vielzahl von Grundstücken“ ist in einem gemeinsamen Gespräch zwischen Vertretern des Berliner Datenschutzbeauftragten, des betroffenen Bezirksamtes und der zuständigen Senatsverwaltung erarbeitet worden.

4.5 Informationsverarbeitung im Dienste von Wissen und Bildung

4.5.1 Wissenschaft und Forschung

Datenschutz als Sündenbock beliebt, aber ungeeignet

Im vergangenen Jahr haben sich mehrere Forschungseinrichtungen und Wissenschaftlervereinigungen wie die Deutsche Forschungsgemeinschaft und die Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften zu *angebli-*

Der Senat teilt die Meinung des Berliner Datenschutzbeauftragten, daß das geltende Datenschutzrecht ausreichend flexible Instrumente bereithält, um zwischen dem informationellen Selbstbestimmungsrecht der betroffenen Menschen und dem

chen Behinderungen oder Blockaden der Forschung durch den Datenschutz geäußert. Allen diesen Stellungnahmen war gemeinsam, daß die geltenden *Forschungsklauseln* in den Datenschutzgesetzen weitgehend außer acht gelassen wurden oder eine noch weiter gehende Privilegierung der wissenschaftlichen Forschung im Datenschutzrecht gefordert wurde.

Es ist nicht zu bestreiten, daß immer wieder datenverarbeitende Stellen, die über den Zugang von Wissenschaftlern zu personenbezogenen Daten zu entscheiden haben, sich hinter den Datenschutz verschanzen oder ihn als *Vorwand* für eine negative Entscheidung benutzen, die in Wirklichkeit auf ganz anderen Gründen (z.B. Kostenüberlegungen) beruht. Demgegenüber ist festzuhalten, daß das geltende Datenschutzrecht (das Berliner Datenschutzgesetz für öffentliche Forschungseinrichtungen, das Bundesdatenschutzgesetz für die Verwendung von privaten Datenbeständen für Forschungszwecke) ausreichend flexible Instrumente bereithält, um zwischen dem informationellen Selbstbestimmungsrecht der betroffenen Menschen und dem Grundrecht der freien Forschung und Lehre zu einem angemessenen Ausgleich zu kommen. Speziell in Berlin mit seinen hohen Forschungskapazitäten ist es nach unserer Kenntnis bisher auch noch nicht zu einem unauflöslichen Konflikt zwischen dem Datenschutz und der Forschungsfreiheit gekommen. Wir beraten Berliner Wissenschaftler seit Jahren ausführlich und intensiv bei der Vorbereitung ihrer Forschungsvorhaben, und dies erweist sich bei der Durchführung dieser Vorhaben später auch als sehr förderlich. Es hat noch nicht einen Fall seit der Ernennung des ersten Berliner Datenschutzbeauftragten im Jahr 1979 gegeben, in dem ein Forschungsvorhaben von diesem insgesamt beanstandet worden wäre. Allerdings haben wir in einer Vielzahl von Fällen Änderungen der Anlage des jeweiligen Forschungsvorhabens empfohlen, um den datenschutzrechtlichen Bestimmungen und vor allem der informationellen Selbstbestimmung des Einzelnen zu entsprechen. Uns ist nicht bekannt, daß ein Wissenschaftler aufgrund unserer Empfehlungen sein Vorhaben aufgegeben hätte. Im Gegenteil haben sich viele Forscher bei uns für die intensive und konstruktive Beratung bedankt.

Auch die Gesetzgebung zum *Krebsregister*, das in der DDR unter eklatanter Verletzung der Patientenrechte errichtet worden war, zeigt, daß ein Ausgleich zwischen diesen Rechten und den Interessen der Forschung für die Zukunft durchaus herstellbar ist. Der Datenschutz hat sich dem Anliegen, diese Datensammlung zu erhalten und in einem mit der ärztlichen Schweigepflicht verträglichen Rahmen fortzuschreiben, nicht verschlossen, sondern hat aktiv an der Erarbeitung dieser neuen Rahmenbedingungen mitgearbeitet[113]. Unsere *Skepsis gegenüber bundesweiten zentralen Krankheitsregistern* bleibt gleichwohl bestehen: Es ist nicht erkennbar, worin der zusätzliche medizinische Wert solcher zentraler Datensammlungen gegenüber Registern zu besonderen Krankheitsformen liegen soll. Die ärztliche Schweigepflicht und die Zweckbindung der für ein bestimmtes Forschungsvorhaben erhobenen Daten gelten auch gegenüber Ärzten und Forschern, die an dem konkreten Behandlungsverhältnis oder Forschungsvorhaben nicht beteiligt waren. Es gilt eben nicht das *„Prinzip des weißen Kittels"*, wonach forschende Ärzte (oder andere Wissenschaftler) ohne weiteres personenbezogene Daten anderen Personen offenbaren dürfen, nur weil sie ebenfalls schweigepflichtig sind oder ein wie auch immer definiertes Forschungsinteresse verfolgen. Zentraler Maßstab ist jeweils die Grundrecht der freien Forschung und Lehre zu einem angemessenen Ausgleich zu kommen. Dies gilt auch hinsichtlich des Krebsregisters und der epidemiologischen Forschung. Auch in diesem Bereich der medizinischen Forschung sind bisher Beschwerden über Behinderungen von Forschungsvorhaben durch datenschutzrechtliche Regelungen oder deren Handhabung nicht bekannt geworden. Dies gilt insbesondere hinsichtlich der Sonderregelung über Datenverarbeitung für wissenschaftliche Zwecke gemäß § 30 des Berliner Datenschutzgesetzes.

In Übereinstimmung mit der Haltung der Bundesregierung zum Bundesdatenschutzgesetz und zur EG-Datenschutzrichtlinie, auf die sich der Datenschutzbeauftragte bezieht, wird auch unsererseits kein aktueller Bedarf für eine Änderung der datenschutzrechtlichen Regelungen zur Erleichterung von medizinischen Forschungsvorhaben gesehen.

[113] JB 1994,4.5

[114] Antwort des Parlamentarischen Staatssekretärs Dr. Waffenschmidt vom 14. September 1996, BT-Drs. 13/5566, S.7

informierte Einwilligung des Betroffenen (Patienten, Befragte); von ihr kann nur unter den engen gesetzlich vorgesehenen Ausnahmen abgesehen werden.

Mit Recht hat es deshalb die Bundesregierung abgelehnt, das Bundesdatenschutzgesetz in dieser Hinsicht zu novellieren, um z.B. eine bessere Grundlage für die epidemiologische Forschung zu schaffen[114]. Ein solcher Änderungsbedarf ergebe sich in diesem Punkt auch nicht aus der EG-Datenschutzrichtlinie von 1995.

Suche nach neuen Wegen

Im Jahresbericht 1995[115] informierten wir über das in Aufbau befindliche *Qualitätssicherungsregister von Dialysepatienten* unter dem Namen QuaSiNiere. Dieses für alle Dialysepatienten mit deren Einwilligung zu errichtende Register bei der Ärztekammer Berlin hat bezüglich des Datenschutzes zwischenzeitlich Modellcharakter erhalten. Zunächst wurde auf unsere Anregung hin zur Anonymisierung bzw. Deanonymisierung der Daten ein Datentreuhänder eingesetzt. Rechtlich war diese Treuhänderfunktion mit Ausnahme des Krebsregisters, das auf einer gesetzlichen Grundlage beruht, nicht abschließend geklärt. Insbesondere ergab sich die Frage, wie sich die rechtliche Stellung des Datentreuhänders mit der ärztlichen Schweigepflicht vereinbaren läßt. Auch war unklar, ob treuhänderisch verwaltete Daten bei einem Anwalt ebenso wie Unterlagen, die der ärztlichen Schweigepflicht unterliegen, oder andere anwaltliche Unterlagen im strafprozessualen Verfahren beschlagnahmefest sind. Die Treuhänderschaft ist ihrem Wesen nach orginäre notarielle oder anwaltliche Tätigkeit. Dies erlaubt es, treuhänderisch Anonymisierungsarbeiten bei einem Anwalt durchzuführen, die bei diesem einer gleichen besonderen Schweigepflicht und Beschlagnahmefestigkeit unterliegen wie beispielsweise bei einem Arzt. Damit sind grundsätzlich Datenspeicherungen möglich, bei denen in anderen Fällen eine Interessenkollision nicht auszuschließen ist. Als Datentreuhänder können ein Anwalt oder ein Notar fungieren, die durch ihre berufliche Tätigkeit keinerlei inhaltliche Eigeninteressen am Datenbestand haben. Dies erlaubt, in Fällen wie dem Register der Dialysepatienten QuaSiNiere unterschiedlichste Interessenlagen zu berücksichtigen und unberechtigte Zugriffe auf personenbezogene Einzeldaten auszuschließen.

Dem Datentreuhänder wurde ein Beirat zur Seite gestellt, der sich aus einem Vertreter der Patientenverbände und einem Arzt zusammensetzt. Dieser ist für die Wahrung der ärztlichen Schweigepflicht beim Datentreuhänder verantwortlich. Dieses scheinbar zunächst komplizierte, in der Realität jedoch durchschaubar und einfach ablaufende Verfahren wurde zwischenzeitlich von vielen Patienten und Einrichtungen akzeptiert. Bei der gegenwärtig noch nicht abgeschlossenen Ersterfassung der Dialysepatienten gaben bislang ca. ¾ der über 40 000 Patienten in Deutschland ihre Einwilligung.

Private Markt- und Meinungsforschung

20.00 Uhr. Das Telefon klingelt. Die Frau des Hauses greift zum Telefon und hört folgendes: „Guten Abend, wir sind vom xyz-Umfrageservice und möchten ihre Meinung zu den politischen Themen dieser Stadt erfahren." Die Frau staunt, ist ihre Nummer doch als Geheimnummer weder im Telefonbuch eingetragen noch über CD-ROM oder die Auskunft der Telekom zugänglich.

[115] JB 1995, 5.14

Einige private Meinungsforschungsinstitute sehen sich zunehmend Zweifeln bezüglich der Repräsentativität ihrer Umfragen ausgesetzt. Um auch Inhaber von Geheimnummern befragen zu können, wurden mit Computern nach Zufallskriterien erzeugte Rufnummern gewählt. Ob dieses Verfahren zu besseren Ergebnissen führt, mag dahingestellt bleiben. Zunächst werden jedoch die angewählten Inhaber von Geheimnummern verunsichert. Wir empfehlen daher von solchen Umfragen betroffenen Bürgern, sich – wenn sie überhaupt teilnehmen wollen – eine Rückrufnummer und die genaue Bezeichnung und Anschrift des Unternehmens geben zu lassen.

Die Post ist da. Ein Umfrageinstitut schreibt direkt mit Namen und Anschrift. Viele Fragen auf einem Bogen zu einem aktuellen politischen Thema. Nun gut, man füllt sie aus. Dabei liegt ein „Rubbellos" und plötzlich hat man einen Auslandsaufenthalt in einem Hotel oder einer Ferienwohnung gewonnen. Was der Gewinner nicht weiß: jedes Rubbellos gewinnt; Nieten gibt es nicht. Das Erwachen kommt allerdings unmittelbar darauf, spätestens am Urlaubsort: Hin- und Rückflug muß der glückliche Gewinner nämlich ebenso selbst bezahlen wie sämtliche Dienstleistungen vor Ort, die über die Kosten der Unterkunft hinausgehen.

Manche Befragungen von „Markt- und Meinungsforschungsinstituten" sind so aufgebaut, daß die „Belohnung" für die Teilnahme an der Umfrage schon gesichert scheint, bevor die Antwort eingegangen ist. In solchen Fällen sind durchaus Zweifel daran angebracht, ob es sich bei dieser Umfrage wirklich um Markt- und Meinungsforschung handelt oder der Zweck nicht vielmehr im Verkauf von Leistungen besteht, die der Befragte zum gleichen Preis (z.B. einer Pauschalreise) auch ohne Offenlegung eigener politischer Auffassungen erhalten könnte. Wir können den Bürgern hier nur ein „gesundes Mißtrauen" empfehlen. Grundsätzlich sollten solche Erhebungen so gestaltet sein, daß der inhaltliche Antwortteil des Fragebogens eindeutig, d. h. auch ohne versteckte Markierungen, Strichcodes oder ähnliches von den Adreßdaten bzw. dem Wunsch auf Teilnahme an einer Verlosung oder einem anderen Gewinnspiel getrennt werden kann. Eine Verquickung von Gewinnspielen und Markt- und Meinungsforschungserhebungen dürfte auch gegen den Grundsatz der Datenerhebung nach Treu und Glauben verstoßen und damit nach Bundesdatenschutzgesetz rechtswidrig sein. Dies gilt dann, wenn der Zweck der Markt- und Meinungsforschung nur vorgeschoben sein sollte, der eigentliche Geschäftszweck aber der eines Reisebüros ist.

4.5.2 Schule

Schulwegbeförderung für Kinder mit Behinderung

Ein wichtiges Ziel der Berliner Schule muß es nach dem Schulgesetz sein, an der *Integration von Kindern mit sonderpädagogischem Förderbedarf* und Behinderung in die Gesellschaft mitzuwirken. In diesem Zusammenhang sei erwähnt, daß die im Jahresbericht 1995 angemahnte Rechtsverordnung für Datenerhebungen und -übermittlungen zur Feststellung des sonderpädagogischen Förderbedarfs nach § 10 a Schulgesetz immer noch aussteht[116]. Das Gebot der Förderung von behinderten Kindern im einzelnen umzusetzen, bedarf es einer Reihe von begleitenden und zum Teil auch kostenaufwendigen Maßnahmen. Dazu gehört, daß Schülern, die wegen ihrer Behinderung nicht imstande sind, die Schule auf dem üblichen Weg zu besuchen, auf Antrag besondere

Nach Novellierung des § 10 a Schulgesetz zur Integration von Schülern mit sonderpädagogischem Förderbedarf im April 1996 (GVBl. S. 126 ff [129]) wird gegenwärtig an einer Rechtsverordnung zur sonderpädagogischen Förderung in der Berliner Schule sowie des dabei zu beachtenden Verfahrens gearbeitet, in dem datenschutzsichernde Regelungen integraler Bestandteil sein werden.

Die Senatsverwaltung für Schule, Jugend und Sport wird das Verfahren zur Schulwegbeförderung von Kindern mit Behinderungen den datenschutzrechtlichen Anforderungen für das Schuljahr 1997/98 anpassen und unter Einbeziehung der Bezirke eine Abstimmung mit dem Datenschutzbeauftragten anstreben.

[116] JB 1995, 5.9

Beförderungsmittel zur Verfügung gestellt werden können. Zwar besteht kein Rechtsanspruch auf diese Leistung, doch wurden in der Vergangenheit die Beförderungsmittel entsprechend dem Grad der Behinderung und der Länge und Dauer des Schulweges großzügig bewilligt.

Nachdem durch eine richterliche Entscheidung festgestellt wurde, daß der Schulweg in den Verantwortungsbereich der Eltern falle, teilte die Senatsschulverwaltung im Jahre 1993 den Bezirken mit, daß diese weitere Gründe für die Gewährung dieser Leistung zu prüfen hätten. Im einzelnen hätten die betroffenen Eltern ihre Berufstätigkeit nachzuweisen bzw. die Verpflichtung, kleinere Geschwister zu betreuen. Auch sollte belegt werden, ob die Eltern im Besitz eines geeigneten eigenen Kraftfahrzeuges sind oder Krankheiten der Eltern eine Begleitung unmöglich machen. Dies sollte durch die Vorlage von Geburtsurkunden, Attesten und anderen Bescheinigungen durch die Erziehungsberechtigten an der Schule geschehen. Die Schule erhielt so Erkenntnisse über die familiären Verhältnisse der Schüler.

Zunächst mußten wir feststellen, daß für diese Datenerhebungen keine Rechtsgrundlage vorhanden war. Die Schulpflichtverordnung sah keine „Zumutbarkeitsprüfung" vor. Unklar blieben auch die Rechtsfolgen. Würde beispielsweise ein behindertes Kind, dessen Eltern die entsprechenden Nachweise nicht erbringen und das somit nicht der Schulpflicht nachkommen kann, zwangsweise der Schule zugeführt werden.

Wir schlugen der Senatsverwaltung für Schule, Jugend und Sport eine Reihe von Maßnahmen einschließlich der Änderung der Schulpflichtverordnung vor, um künftig ein für alle Bezirke gleiches und datenschutzgerechtes Verfahren der Bewilligung dieser zusätzlichen öffentlichen Leistungen einzuführen.

Schülerausweise im Scheckkartenformat vom Schulfotografen

Jede Schulsekretärin weiß, wie zeitaufwendig zu Beginn des Schuljahres das Erstellen von Schülerausweisen sein kann. Häufig füllen die Schüler die Ausweisvordrucke selbst aus, lassen sie vom Lehrer abzeichnen und im Schulsekretariat stempeln. Auch dies ist ein Aufwand, aber ohne Schülerausweis kann so manche Ermäßigung nicht in Anspruch genommen werden. Um so mehr freuten sich einige Schulen über das vom Landesschulrat unterstützte Angebot von Fotofirmen, neben den zu bezahlenden Klassenfotos und Einzelporträts kostenlos Schülerausweise anzufertigen.

Zunächst baten die Fotofirmen die Schulen, ihnen *Klassenlisten* mit Namen, Geburtsdatum und Anschrift zu übergeben. Nach dem Fotografieren wurde der Schule für jeden Schüler ein den Verwaltungsvorschriften entsprechender Schülerausweis mit Bild des Schülers zur Verfügung gestellt. Auch wenn in dem Begleitschreiben des Landesschulrats auf die einschlägigen datenschutzrechtlichen Bestimmungen verwiesen wurde, war dieses Verfahren so nicht rechtmäßig.

Bei dem zunächst praktizierten Verfahren stellt die Übermittlung der Klassenlisten an eine nicht-öffentliche Stelle einen erheblichen Verstoß gegen § 5a Abs. 3 Schulgesetz dar. Danach ist eine Übermittlung nur mit Einwilligung oder bei Vorliegen einer Rechtsgrundlage zulässig. Wir empfehlen der Senatsverwaltung, dem Landesschulamt und seinen Außenstellen sowie den Schulen, die Situation durch klare vertragliche Regelungen, die insbesondere eine Speicherung der Schülerdaten bei den Unternehmen ausschließen, zu bereinigen.

Die von den einzelnen Fotofirmen praktizierten Verfahren zur Herstellung von Schülerausweisen im Scheckkartenformat sind und waren rechtlich zulässig.

Gemäß Nr. 1 Abs. 1 der Ausführungsvorschriften über Schülerausweise vom 14. März 1991 (ABl. S. 635, DBl. III S. 39) erhalten Schülerinnen und Schüler der Berliner Schulen von ihrer Schule auf Antrag einen Schülerausweis. Mit der Antragstellung in der Schule geben die Schülerinnen und Schüler, im Falle der Grundschüler die Erziehungsberechtigten, die Einwilligung zur Verarbeitung ihrer personenbezogenen Daten durch die Schule. Die vom Berliner Datenschutzbeauftragten kritisierte fehlende Einwilligung der Schülerinnen und Schüler bzw. der Erziehungsberechtigten zur Verarbeitung von personenbezogener Daten lag demnach vor.

Auch die Weitergabe der Schülerdaten durch die Schule an Dritte, hier die Fotofirmen, ist rechtlich nicht zu beanstanden. Nach § 1 Abs. 2 S. 2 Schuldatenverordnung vom 13. Oktober 1994 (GVBl. S. 435) sind Schulen datenverarbeitende Stellen im Sinne des Berliner Datenschutzgesetzes. Aus diesem Grund sind die einzelnen Schulen berechtigt, die Verarbeitung

personenbezogener Daten im Wege der Auftragsdatenverarbeitung auch nicht-öffentlichen Stellen zu überlassen. Das Verfahren zur Verarbeitung der Daten im Auftrag ist in § 3 Berliner Datenschutzgesetz geregelt. Danach liegt eine Auftragsdatenverarbeitung vor, wenn sie ausschließlich im Rahmen der Weisung des Auftraggebers erfolgt. In unserem Genehmigungsschreiben wird ausdrücklich darauf hingewiesen, daß der Schulleiter über die Anfertigung der Fotos und Schülerausweise entscheidet. Mit seiner Entscheidung erhält die jeweilige Firma vom Schulleiter die Bestätigung/den Auftrag, die Schülerausweise anzufertigen und die Daten dabei gemäß seinen Weisungen zu verarbeiten. Gleichzeitig sind die anbietenden Firmen durch unsere Genehmigungsschreiben verpflichtet, die im Land Berlin geltenden datenschutzrechtlichen Bestimmungen einzuhalten. Einen Verstoß gegen die Bestimmungen des § 3 Berliner Datenschutzgesetz oder § 5 a Schulgesetz (SchulG) vermögen wir in dem bisher praktizierten Verfahren nicht zu erkennen. Gleichwohl haben wir uns, um für die Schulen die erforderliche Rechtssicherheit zu schaffen, unverzüglich mit dem Berliner Datenschutzbeauftragten und den anbietenden Firmen in Verbindung gesetzt und ein mit allen Beteiligten abgestimmtes Verfahren festgelegt, über das die Schulen mittels Rundschreiben informiert werden.

Datenschutz im Internat

„Als Mädchen würde ich mich schämen, in diesem Dreck zu leben! Sofortige Änderung! Der Leiter". Zettel dieser Art hinterließ der Leiter eines Internats nach einem „Stubendurchgang". Die Schülerinnen waren nicht anwesend. Zutritt zu den Internatswohnungen verschaffte sich der Internatsleiter mit einem Generalschlüssel.

Im vergangenen Jahr wurden wir gebeten, uns mit datenschutzrechtlichen Problemen des *Internatslebens* zu beschäftigen. Einige Berliner Schulen geben Jugendlichen auf Grundlage von Verträgen mit den Erziehungsberechtigten die Möglichkeit, in einem Internat zu wohnen. Internat und Schule sind jedoch in keiner Weise datenschutzrechtlich gleichzusetzen. Durch den Internatsvertrag übertragen die Eltern Rechte aus ihrer Personensorge der Schule als Internatsträger. Damit ist nicht das Schulgesetz Grundlage der Tätigkeit der Erzieher im Internat, sondern dieser Vertrag und als dessen Bestandteil die Internatsordnung. Für das Internat ist die Verarbeitung personenbezogener Daten nur im Rahmen der Zweckbestimmung des Vertragsverhältnisses zulässig (§ 28 Abs. 1 BDSG). Die Beziehung zwischen Internat in Vertretung der Erziehungsberechtigten und der Schule richtet sich wiederum nach dem Berliner Schulrecht.

Eine *Internatswohnung* oder ein Internatszimmer ist eine Wohnung im Sinne des Artikel 13 Grundgesetz. Sie muß auch dem Internatsbewohner einen unantastbaren Bereich privater Lebensgestaltung erlauben, einen Bereich, in den sich der Einzelne zurückziehen kann, niemand ohne Zustimmung des Bewohners Zutritt hat, in dem man in Ruhe gelassen wird und auch ein Recht auf Einsamkeit genießt[117]. Diese Grundsätze müssen auch für grundrechtsmündige (etwa ab dem 14. Lebensjahr) und abgestuft für jüngere Internatsbewohner gelten. Dabei ist das wachsende Bedürfnis der Heranwachsenden zu selbständigem verantwortungsbewußten Handeln zu berücksichtigen, das den Entscheidungsspielraum der Personensorge fortschreitend einschränkt (§ 1626 Abs. 2 Bürgerliches Gesetzbuch). Datenschutzrechtlich ist das Eindringen in eine Wohnung in jedem Fall mit einer Datenerhebung über die

Die Problematik war in der Vergangenheit Gegenstand zahlreicher Erörterungen zwischen dem Berliner Datenschutzbeauftragten und dem Landesschulamt Berlin, die noch nicht abgeschlossen sind. Auf die Bereitschaft des Berliner Datenschutzbeauftragten, an der Lösung der Probleme mitzuwirken, wird das Landesschulamt Berlin zurückgreifen.

[117] siehe BVerfGE 27,1, 6

Persönlichkeitssphäre oder sogar die Intimsphäre des Betroffenen verbunden.

Daher forderten wir, durch die Internatsordnung hier klare Regeln zu schaffen. So ist festzulegen, zu welchem Zwecken die Erzieher, welchen die elterliche Sorge während des Internatsaufenthaltes übertragen ist, befugt sind, Wohnungen bzw. Zimmer von Internatsbewohnern zu betreten. Im Regelfall dürfte die normale tägliche Betreuung durch die Erzieher hinreichend sein, die übertragenen Aufsichts- und Erziehungsfunktionen sowie die Fürsorgepflicht und die Ordnungsfunktionen wahrzunehmen. Insbesondere sollte eine Besichtigung der Räume grundsätzlich nur in Anwesenheit der Schüler erfolgen.

Auch bezüglich der Registrierung von An- und Abmeldungen, Ausgängen, Urlaub im Internat schlugen wir ein Verfahren vor, das es ausschließt, Verhaltensprofile der Bewohner zu erkennen und zu speichern. Wir betonten gegenüber dem Landesschulamt unsere Bereitschaft, aus datenschutzrechtlicher Sicht an einer Rahmenordnung für die Internate mitzuwirken.

4.5.3 Statistik

Volkszählung 2001, 2002, 2003 ...?

Unweit der Dienststelle des Berliner Datenschutzbeauftragten prangt mit schwarzen Lettern an eine Häuserwand gesprüht „Volkszählun(g)sboykott". Ein Überbleibsel aus einer Zeit, die wegen des Volkszählungsurteils des Bundesverfassungsgerichtes für den Datenschutz sehr bewegt war. Mittlerweile sind die Ergebnisse der letzten Volkszählung schon in die Jahre gekommen. Die Daten aus der letzten Zählung für die alte Bundesrepublik sind jetzt 10 Jahre alt und die für die ehemalige DDR 16 Jahre. Unstrittig war im Volkszählungsurteil von 1983, daß der Staat und viele andere für künftiges Planen und Handeln periodisch aktuelle Daten benötigen.

Die 1987 nach dem Volkszählungsurteil erneut durchgeführte Volkszählung als Totalerhebung war nach Auffassung der Statistiker zum damaligen Zeitpunkt durch keine *mildere Form des Eingriffs* in das informationelle Selbstbestimmungsrecht zu ersetzen. Das Bundesverfassungsgericht hatte allerdings festgestellt: „Vor künftigen Entscheidungen über eine Erhebung wird sich der Gesetzgeber erneut mit dem dann erreichten Stand der Methodendiskussion auseinandersetzen müssen, um festzustellen, ob und in welchem Umfang die herkömmlichen Methoden der Informationserhebung und -verarbeitung beibehalten werden können... Es reicht insoweit zur Begründung nicht aus, lediglich darauf zu verweisen, daß Volkszählungen schon immer in Form von Totalerhebungen durchgeführt worden seien."[118]

Statistiker schätzen, daß bei einer jetzt einsetzenden Vorbereitung einer Volkszählung diese frühestens im Jahre 2003 stattfinden könne. Insbesondere von der Europäischen Union wird jedoch erwartet, daß die Mitgliedstaaten etwa um das Jahr 2001 aktuelle Volkszählungsdaten erheben, die dann auch Grundlage für die Vergabe von EU-Mitteln sein werden. Die somit absehbare mißliche Situation veranlaßte im Herbst 1996 das Bundesministerium des Innern, Probleme und Lösungsansätze zu skizzieren.

Die auf einige Milliarden D-Mark geschätzten Kosten einer erneuten *Totalerhebung* scheinen diese Variante auszuschließen. Eine Nutzung der Melderegister als anderer Weg dürfte zum einen die Informationsbedürfnisse einer

Es wird geprüft, ob durch Auswertungen aus den Melderegistern und aus anderen verfügbaren amtlichen Datenwerken Ersatzlösungen für einen Zensus erarbeitet werden können. Hierbei hat sich herauskristallisiert, daß auf diesem Wege womöglich den Datenanforderungen der Europäischen Union – wenn auch nicht vollständig – und den Informationsbefürfnissen auf Bundesebene entsprochen werden könnte.

Entgegen dem Eindruck des Berliner Datenschutzbeauftragten hat das Statistische Bundesamt intensive Beratungen über alternative Erhebungsverfahren durchgeführt, an denen das Statistische Landesamt Berlin wie auch die Statistischen Landesämter maßgeblich beteiligt waren.

[118] BVerfGE 65, S. 55 ff.

Volkszählung nicht decken und zum anderen ohne vorherige Bereinigung eine sehr hohe Fehlerquote beinhalten. Zwar erhält das Statistischen Landesamt auf Grundlage einer Rechtsverordnung und des Landesstatistikgesetzes monatlich einen anonymisierter Abzug des Melderegisters und wertet diesen für die Bevölkerungsfortschreibung aus. Informationen wie die Zahl und Struktur der Haushalte, Angaben zur Erwerbstätigkeit sowie zum Pendlerverhalten lassen sich aus dem Melderegister jedoch nicht gewinnen.

Der Vorschlag, in einer durch Bundesgesetz vorgeschriebenen Kampagne die Melderegister zu bereinigen, zusätzliche nur für Zwecke der Statistik benötigte Angaben zu erheben und zu speichern, ist allerdings außerordentlich bedenklich. Die verfassungsrechtlich geforderte Trennung von Statistik- und Verwaltungsvollzug würde so verwischt werden. Insbesondere stünde zu erwarten, daß die neuaufzunehmenden Daten des Melderegisters auch andere, nichtstatistische Begehrlichkeiten zu ihrer Nutzung wecken. Das Vorhalten und die ständige Aktualisierung eines mit vielen statistischen Merkmalen angereicherten Melderegisters bringt die Gefahr einer persönlichkeitsfeindlichen Registrierung und Katalogisierung des Einzelnen mit sich. Für eine im Zehnjahresabstand erfolgende statistische Auswertung des Registers würden dann dauerhaft Persönlichkeitsprofile gespeichert.

Es scheint, als seien die vergangenen Jahre von der amtlichen Statistik nicht hinreichend genutzt worden, die Möglichkeiten einer Kombination von Voll- und Stichprobenerhebung mit einem größeren Anteil *freiwillig* zu beantwortender Fragen konsequent zu prüfen und als Alternative für die Totalerhebung zu entwickeln.

Ob angesichts der bundesweit extrem knappen Ressourcen auf allen Ebenen ein Zensus überhaupt und mit welchen Methoden und welchem Inhalt durchgeführt werden wird, ist derzeit offen.

4.6 Information als Wirtschaftsgut: Datenverarbeitung in der Privatwirtschaft

4.6.1 Banken und Versicherungen

Wertpapierhandelsgesetz

Bereits im Vorjahr ist berichtet worden, daß die datenschutzrechtliche Brisanz von § 31 Abs. 2 Wertpapierhandelsgesetz offensichtlich unterschätzt worden war. Diese Vorschrift verpflichtet die Bank, „von ihren Kunden Angaben über ihre Erfahrungen oder Kenntnisse in Geschäften, die Gegenstand von Wertpapierdienstleistungen sein sollen, über ihre mit den Geschäften verfolgten Ziele und über ihre finanziellen Verhältnisse zu erlangen." Um dieser Norm zu entsprechen, haben verschiedene Banken von den Anlegern die Ausfüllung umfangreicher Fragebogen verlangt, die entgegen der gesetzlichen Vorgabe keine produkt- und kundenbezogenen Differenzierungen enthielten[119].

In der Sitzung der Obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich mit dem Zentralen Kreditausschuß im April 1996 wurde von Vertretern beider Seiten die Hoffnung geäußert, daß eine *Richtlinie des Bundesaufsichtsamtes für den Wertpapierhandel* dazu beitragen würde, die aufgetretenen datenschutzrechtlichen Probleme zu klären. Der erste vorgelegte Entwurf des Bundesaufsichtsamtes enttäuschte diese Hoffnung. Das Bundesaufsichtsamt begnügte sich mit der Erwartung, daß den Banken das Bundesdatenschutzgesetz bekannt sei und deshalb keine genaueren Angaben zum Umfang der Kundenangaben erforderlich seien. Die Kritik des Berliner Datenschutzbeauftragten und der anderen Aufsichtsbehörden in der schriftlichen und mündlichen Anhörung zu der

[119] JB 1995, 6.3

beabsichtigten Richtlinie führte dazu, daß der Entwurf in wesentlichen Punkten verbessert wurde. Insbesondere wurde klargestellt, daß die Bank nur verpflichtet ist, von dem Kunden Angaben über die von ihm verfolgten Anlageziele, über seine Kenntnisse oder Erfahrungen in den einzelnen Anlageformen und über seine finanziellen Verhältnisse zu verlangen, *soweit dies erforderlich ist*. Der Umfang der vom Kunden einzuholenden Angaben ist am Interesse des Kunden und an Art und Umfang der beabsichtigten Geschäftsarten auszurichten. Der Entwurf akzeptiert zwar die Verwendung von Fragebögen, durch die jetzt erfolgte Erwähnung des Erforderlichkeitsprinzips dürfte aber klargestellt sein, daß standardisierte Fragebögen nur dann Verwendung finden können, wenn sie eine produktbezogene Differenzierung ermöglichen.

Der neue Richtlinienentwurf (mit dem Inkrafttreten ist 1997 zu rechnen) stellt außerdem klar, daß die Bank sicherstellen muß, daß sie die erhaltenen Angaben ausschließlich für die Zwecke der Aufklärung und Beratung des Kunden verwendet, es sei denn, der Kunde stimmt einer anderweitigen Verwendung ausdrücklich zu.

Noch offen ist, ob das Aufsichtsamt unsere Forderung erfüllen wird, die Wertpapierdienstleistungsunternehmen zu verpflichten, den Kunden darauf hinzuweisen, daß für ihn keine gesetzliche Verpflichtung besteht, Angaben zu machen. Unserem Wunsch, daß die Richtlinie den Wertpapierdienstleistungsunternehmen klarere Vorgaben zu den bei den einzelnen Produkten jeweils notwendigen Angaben (differenziert nach Anlageziel, Kenntnissen bzw. Erfahrungen, finanziellen Verhältnissen) geben sollte, wurde nicht entsprochen. Die sehr abstrakte Darstellung des Erforderlichkeitsprinzips der Richtlinie wird deshalb in der Praxis dazu führen, daß in konkreten Einzelfällen weiterhin fraglich bleibt, welche Angaben erhoben werden dürfen.

Familiengründungsdarlehen

Die Berliner Sparkasse hat Jugendlichen zu ihrem 13. Geburtstag gratuliert. Der Glückwunsch war mit der Einladung verbunden, einmal die örtlich zuständige Sparkassenfiliale aufzusuchen und dort Tips und Antworten auf Fragen zum Geld zu erhalten. Besonders makaber war, daß die Sparkasse in einem Fall einem Jugendlichen zu seinem 13. Geburtstag gratuliert hatte, der im Alter von 3 Monaten verstorben war.

Der Senat von Berlin hatte 1961 mit der Sparkasse der Stadt Berlin-West eine Vereinbarung über die Gewährung von *Familiengründungsdarlehen* aus Landesmitteln getroffen. Die Sparkasse hatte in der Vereinbarung die Gewährung der Familiengründungsdarlehen nach den dort geregelten Grundsätzen übernommen. Die Darlehensnehmer mußten unter anderem bei der Sparkasse die Geburtsurkunden ihrer Kinder einreichen. Daraus stammten die Daten.

Da es sich bei den Familiengründungsdarlehen um vom Land Berlin gewährte Gelder gehandelt hat, war nach der Vereinbarung allein die Berliner Sparkasse für die Gewährung und Verwaltung der für die Auszahlung der Darlehen zur Verfügung gestellten Landesmittel zuständig. Aus diesem Grunde konnte die Leistung „Familiengründungsdarlehen" nur von der Berliner Sparkasse erbracht werden. Da die Berliner Sparkasse nicht als Wettbewerber Leistungen erbrachte, die auch von privaten Anbietern hätten erbracht werden können, ist ihr Verhalten nach den schärferen Vorgaben des Berliner Datenschutzgesetzes zu messen. Die zum Zwecke der Vergabe und Verwaltung der Darlehen erhobenen Daten unterliegen daher der Zweckbindung des § 11 Abs. 1 und 2 BlnDSG. Danach dürfen personenbezo-

Die Landesbank Berlin hat hierzu mitgeteilt, daß die Angelegenheit zwischenzeitlich erledigt ist. Erhobene Daten werden nur noch im Rahmen der gesetzlichen Aufbewahrungsfristen gespeichert, eine weitere Verwendung erfolgt nicht. Der Datenschutzbeauftragte ist vom Institut in Kenntnis gesetzt worden.

gene Daten grundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben oder gespeichert worden sind. Dies schließt eine Verwendung der Daten zu Werbezwecken aus.

„Postverbot"

Jeder Bürger hat die Möglichkeit, gegenüber Privatunternehmen der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung zu widersprechen. Nach erfolgtem Widerspruch ist die Nutzung oder Übermittlung für diesen Zweck unzulässig.

Nachdem eine Bankkundin von ihrem Widerspruchsrecht Gebrauch gemacht hatte, erhielt sie von ihrer Bank keinerlei Post mehr, auch keine Kontoauszüge oder sonstige für einen Bankkunden relevanten Informationen. Eine Versendung von Kontoauszügen sei nicht möglich, da auf diesen kurze Werbetexte enthalten seien.

Das Verhalten der Bank ist rechtswidrig. Es führt zu dem Ergebnis, daß Bankkunden nur dann die vertragliche Leistung, durch *Kontoauszüge* über ihren Kontostand informiert zu werden, erhalten, wenn sie bereit sind, auf ihr Recht aus § 28 Abs. 3 BDSG zu verzichten. Durch ein derartiges Junktim wird der Wille des Gesetzgebers, jedem Bürger ein Widerspruchsrecht gegen Werbemaßnahmen einzuräumen, umgangen.

Während unserer Verhandlungen mit der Bank stellte sich heraus, daß nur zehn Kunden ein Werbeverbot ausgesprochen hatten. Die Bank teilte uns mit, daß sie nicht in der Lage sei, kurzfristig zehn Bankkunden mit werbefreien Kontoauszügen zu bedienen. Sie versprach allerdings, 1997 durch eine entsprechende Softwareänderung ein differenziertes Postversendungsverfahren einzuführen. Bis dahin müssen sich die Bankkunden ihre werbefreie Post in ihrer Bankfiliale abholen.

Mitarbeiterleitsätze

Kritik übten wir an der Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen über Anforderungen an *Regelungen der Kreditinstitute für Mitarbeitergeschäfte* vom 30. Dezember 1993. Nach den Vorgaben dieser Verlautbarung sollen die Kreditinstitute ihre Mitarbeiter verpflichten, auf Verlangen vollständige Auskunft über ihre Mitarbeitergeschäfte (alle Geschäfte, die der Mitarbeiter außerhalb seiner dienstlichen Aufgabenstellung für eigene Rechnung oder für Rechnung Dritter tätigt) zu erteilen. Die Auskunftspflicht bezieht sich auch auf Mitarbeitergeschäfte, die er als Bevollmächtigter, als Testamentsvollstrecker oder in ähnlicher Funktion tätigt. Die Auskunftsverpflichtung besteht auch, wenn das Geschäft nicht über die eigene Bank bzw. Sparkasse abgewickelt wurde.

Grundsätzlich ist nicht zu bezweifeln, daß Einschränkungen des informationellen Selbstbestimmungsrechts der Mitarbeiter (zumindest teilweise) notwendig sind, um sicherzustellen, daß Mitarbeitergeschäfte nicht gegen Kundeninteressen oder gegen Eigeninteressen der Banken gerichtet sind. Allerdings wäre es aus datenschutzrechtlicher Sicht besser, wenn dies in einem bereichsspezifischen Arbeitnehmerdatenschutzgesetz geregelt werden würde.

Auch inhaltlich bereitet die Verlautbarung Probleme. So regelt sie nicht, welche Bankmitarbeiter nicht unter die Verlautbarung fallen, weil eine Gefährdung der Kunden oder des Kreditinstituts von vornherein ausgeschlossen ist (z.B. Kassierer, Berater für Unternehmensgründungen, Schreibkräfte.).

Insbesondere ist es problematisch, daß die Mitarbeiter der Banken verpflichtet sind, Geschäfte, die sie für *Rechnung*

Dritter abschließen, ihrem Arbeitgeber zu offenbaren. Dies gilt insbesondere dann, wenn der Dritte sein Depot in einer anderen Bank führt. Der Mitarbeiter muß vom Vollmachtgeber bei der Übernahme der Vollmacht das Einverständnis für die Offenlegung einholen. Bei einem durch Rechtsgeschäft zustande gekommenen Vertretungsverhältnis (§§ 164 ff. BGB) muß der Betroffene schriftlich einwilligen (§ 4 Abs. 2 BDSG). Den Weg über eine Einwilligung wird man bei gesetzlichen Vertretungsverhältnissen allerdings nicht gehen können. Im Verhältnis zwischen Testamentsvollstrecker und Erbe ist der Vollmachtgeber der verstorbene Erblasser. Auch bei minderjährigen Kindern kann kein Einverständnis für die Offenlegung von Mitarbeitergeschäften eingeholt werden. Noch problematischer ist der Fall der Betreuung. Gem. § 1898 BGB kann auch ein Bankmitarbeiter verpflichtet werden, eine Betreuung zu übernehmen. Die bei der rechtsgeschäftlichen Vollmachterteilung eingebauten Sicherungen des informationellen Selbstbestimmungsrechts (Einholung einer Einverständniserklärung) haben bei derartigen Vertretungsverhältnissen keine Wirkung. Um das informationelle Selbstbestimmungsrecht der gesetzlich Vertretenen gleichwohl zu gewährleisten, haben wir gegenüber dem Bundesamt den Vorschlag gemacht, daß die Bankmitarbeiter die Möglichkeit erhalten, die nach der Verlautbarung vorzulegenden Geschäfte für Dritte, bei denen kein rechtsgeschäftliches Vertretungsverhältnis vorliegt, zu anonymisieren. Gegen unseren Vorschlag hat das Bundesamt keine Bedenken erhoben.

Telekom-Emission

Der Börsengang der Telekom AG ist nicht nur an den Finanzmärkten mit großer Aufmerksamkeit verfolgt worden, es entstanden auch datenschutzrechtliche Probleme. Offensichtlich erstmals bei der Emission einer deutschen Aktie wurden Kleinanlegern *Incentives* (Preisnachlaß und Treueaktien) gewährt. Da pro Anleger nur 300 Aktien incentive-begünstigt waren, wurde mit Hilfe einer Wirtschaftsprüfungsgesellschaft gewährleistet, daß kein Anleger – auch wenn er bei verschiedenen Banken über Konten verfügt – über den festgesetzten Höchstbetrag hinaus Incentives erhält. Um der Wirtschaftsprüfungsgesellschaft die Überprüfung zu ermöglichen, wurden dem Treuhänder Name, Vorname, Anschrift und Geburtsdatum des die Vergünstigung in Anspruch nehmenden Anlegers übermittelt sowie die Möglichkeit der Einsichtnahme in die Kaufverträge eingeräumt.

Wegen der Bedeutung des Bankgeheimnisses wäre es geboten gewesen, daß diese Datenübermittlung nur mit Einwilligung des betroffenen Bankkunden erfolgt wäre. Entgegen der Darstellung aus Konsortialkreisen wäre die Einholung einer Einwilligung auch praktisch durchführbar gewesen, da entgegen den Befürchtungen der Banken bei einer telefonischen Aktienbestellung die Einwilligungserklärung mündlich hätte erteilt werden können. Die Einwilligung bedarf nur dann der Schriftform, soweit nicht wegen besonderer Umstände (z.B. telefonischer Kontakt) eine andere Form angemessen ist.

Immerhin gelang es den Aufsichtsbehörden, die Konsortialführer davon zu überzeugen, daß zumindest jeder einzelne Kunde über die Datenübermittlung an den Treuhänder informiert wurde. Es wurde zugesagt, daß auch bei jeder telefonischen Auftragserteilung dem Kunden ein entsprechender Hinweis gegeben wird. Dieses Verfahren erscheint uns gerade noch datenschutzrechtlich vertretbar, da durch den Hinweis im Kaufantrag die Datenübermittlung an den Treuhänder zum Vertragsgegenstand wird.

Gruppenversicherungsverträge

Einige deutsche Versicherungen versuchen, Kunden durch Gruppenversicherungsverträge zu akquirieren. Gruppenversicherungsverträge enthalten gegenüber Einzelverträgen in der Regel Vergünstigungen (z.B. geringere Prämie, keine Gesundheitsüberprüfung). Als Versicherungsnehmer von Gruppenversicherungsverträgen kommen insbesondere Mitglieder von Verbänden und Vereinen (z.B. Seniorenvereine) in Betracht. Die Versicherungen wenden sich deshalb an diese Einrichtungen und bitten sie um die Herausgabe ihrer Mitgliedslisten. Wenn die Vereine und Verbände ihnen die personenbezogenen Daten ihrer Mitglieder (Name, Anschrift, Geburtsjahr) übermitteln, schreiben die Versicherungen die Mitglieder an und bieten ihnen den Abschluß eines Gruppenversicherungsvertrages (in der Regel mit einem Hausbesuch verbunden) an. An dem Abschluß von Gruppenversicherungsverträgen haben in der Regel auch die Verbände und Vereine ein Interesse, da diese nunmehr an ihre Mitglieder herantreten und sie bitten, die durch den Gruppenversicherungsvertrag eingetretenen Vergünstigungen (Differenz zwischen dem höheren Beitrag eines Einzelvertrages und dem Beitrag des Gruppenversicherungsvertrages) an sie abzutreten.

Bereits im Jahr 1990 wurde zwischen den Aufsichtsbehörden für den Datenschutz und der Versicherungswirtschaft eine Absprache über Gruppenversicherungsverträge getroffen. Danach legen *Vereine*, die ihren Mitgliedern die Teilnahme an Gruppenversicherungsverträgen ermöglichen wollen, diesen mit der Beitrittserklärung zugleich eine Einwilligungserklärung zur Datenübermittlung vor, deren Unterzeichnung freiwillig ist. Die Vereinbarung betraf nur Neumitglieder.

Bei einer Überprüfung in einem Einzelfall stellten wir fest, daß die Versicherung die Vereinbarung seit 7 Jahren nicht eingehalten hatte. Die Mehrzahl der Vereine hätte sich geweigert, ihren neuen Mitgliedern neben der Beitrittserklärung eine zweite Unterschrift für die datenschutzrechtliche Einwilligungserklärung abzuverlangen. Deshalb sei das vereinbarte Verfahren nie praktiziert worden. Statt dessen wurden die Neumitglieder über die geplante Datenübermittlung an die Versicherung lediglich informiert mit dem Hinweis, daß dasjenige Mitglied, das diese nicht wünscht, Widerspruch einlegen muß. Der vorliegende Fall wirft die Frage auf, welchen Sinn mehrjährige Verhandlungen mit der Versicherungswirtschaft haben, wenn diese getroffene Vereinbarungen anschließend nicht einhält.

Die „unfehlbare" Bankautomation

Bereits im September 1995 berichtete uns ein Kunde der Berliner Sparkasse, er habe versehentlich seine Eurocheque-Karte eines schleswig-holsteinischen Kreditinstituts in einen Geldausgabeautomaten der Berliner Sparkasse gesteckt, aber die persönliche Identifikationsnummer (PIN) seiner Eurocheque-Karte für die Berliner Sparkasse benutzt. Er habe dennoch anstandslos den gewünschten Betrag erhalten. Ihn erregte jedoch besonders, daß seine sofortige Mitteilung an Mitarbeiter der Sparkassenfiliale, zu der der Automat gehörte, sowie ein Telefax an die Sparkassenzentrale nicht ernst genommen worden waren. Er habe sich Zeugen gesucht und den Vorgang zu einem anderen Zeitpunkt wiederholt. Er habe ferner die Redaktion eines Wirtschafts-Fernsehmagazins über den Vorfall informiert, das sich sehr interessiert gezeigt habe.

Erst nachdem wir nach dem Anruf des Sparkassenkunden die behördliche Datenschutzbeauftragte der Berliner Sparkasse

baten, sich mit den Angaben des Kunden zu befassen, prüfte die Sparkasse den Vorfall und fand die Angaben des Kunden bestätigt. Es war aber zu spät, um die Veröffentlichung im Fernsehmagazin zu verhindern. Zu den Ursachen des Vorfalls konnte die Sparkasse nur die Vermutung äußern, daß der Fehler im Zusammenhang mit der kurz zuvor erfolgten Einführung des *Nationalen Online-Verbundes* stand, der es ermöglicht, daß jede Abfrage des Verfügungsrahmens und der PIN bei einer Geldautomatenabhebung in Deutschland direkt am Konto durchgeführt wird, so daß die Betragsgrenzen für solche Abhebungen wesentlich erhöht werden konnten. Eine nähere Untersuchung war der Sparkasse nicht möglich, weil der Kunde nicht bereit war, die Eurocheque-Karte zur Prüfung herauszugeben.

Nachdem die erste Sendung kein wesentliches Echo gefunden hatte, sorgte der Fall im November 1996 für dicke Schlagzeilen in der Boulevardpresse und für eine weitere Fernsehsendung. In der Zwischenzeit hatten namhafte Fachleute anhand der Untersuchung der Eurocheque-Karte festgestellt, daß ein Softwarefehler die Ursache für den Vorfall sein mußte.

In einer erneuten Stellungnahme versicherte die Sparkasse, daß es sich um einen Sonderfall gehandelt habe. Die Karte des Kunden von der schleswig-holsteinischen Bank habe einen Fehler gehabt, der zwar normalerweise zur Rückweisung der Karte geführt hätte, in diesem Falle aber nicht, weil der benutzte Geldautomat älteren Typs wegen eines Fehlers die *PIN-Prüfung* durch das Rechenzentrum der schleswig-holsteinischen Bank nicht veranlaßt hatte, somit die PIN-Prüfung auch nicht erfolgte. Die Berliner Sparkasse betonte, daß die Fehlfunktion nur beim gleichzeitigen Auftreten des Karten- und des Geldautomatenfehlers erfolgen konnte. Dies hätte zwar noch in anderen Fällen passieren können, jedoch seien keine weiteren einschlägigen Reklamationen bekanntgeworden. Der Softwarefehler der Geldautomaten war im Oktober 1995 behoben worden.

Der Fall bestätigt die informatische Binsenweisheit, daß es keine fehlerlosen Systeme gibt. Insofern könnte man zur Tagesordnung übergehen. Allerdings ist die Sparkasse wie andere Kreditinstitute davon ausgegangen, daß die Geldautomatensysteme so sicher sind, daß es dem Kunden überlassen bleiben kann, das Gegenteil zu beweisen, wenn er unberechtigte Abhebungen an seinem Konto reklamieren will. Kann er dies nicht, kann seine Reklamation als Betrugsversuch angesehen und entsprechend angezeigt werden. Eine solche Umkehrung der Beweislast, die sich auf die Annahme stützt, die Banksysteme seien sicher, erscheint nicht mehr vertretbar.

Die Selbstbedienungssysteme der Kreditinstitute weisen auch andere technisch-organisatorische Schwachstellen auf, die dem Stand der Technik nicht entsprechen:

Wird eine Karte nach *Ablauf ihrer Geltungsdauer* durch eine neue ersetzt, bleibt die gleiche vierstellige numerische PIN gültig. Wenn man sich also nicht außer der Reihe eine neue Karte geben läßt, z.B. im Falle eines Verlustes, also keine Änderung der Kartenfolgenummer die Änderung der PIN bewirkt, kann es sein, daß man die gleiche PIN über viele Jahre behält. Das Phänomen der Paßwortalterung, wonach sich mit zunehmender Geltungsdauer eines Paßwortes die Wahrscheinlichkeit erhöht, daß es Unbefugten zur Kenntnis gelangt ist, wird dabei ignoriert. Dabei gibt es viele Gelegenheiten, die PIN Dritten unbeabsichtigt zu offenbaren, denn viele Geschäfte, in denen Diskretionszonen an den Kassen nicht üblich sind, verwenden bargeldlose Zahlungsverfahren unter Verwendung von Scheck- oder Bankkarten in Verbindung mit der PIN.

Für die Nutzung von *Kontoauszugsdruckern* benötigt man überhaupt keine PIN. Wenn man seine Karte verliert, muß man damit rechnen, daß sich Unbefugte über die letzten Umsätze, den Kontostand und eingeräumten Dispositionskredit informieren. Dies bedeutet zwar nicht, daß man ärmer wird, aber daß die Daten, die immerhin dem Bankgeheimnis unterliegen und deren Offenbarung schutzbedürftige Interessen der Betroffenen möglicherweise nicht nur abstrakt beeinträchtigt, Unbefugten bekannt werden. Empfehlungen, die zu Änderungen dieses Zustandes führen würden, also z.B. die Eingabe der PIN auch bei Kontoauszugsdruckern, wurden vom Zentralen Kreditausschuß mit dem Hinweis abgewiesen, dies sei nicht kundenfreundlich.

4.6.2 Auskunfteien

Überprüfung

Wir führten eine Überprüfung bei einer der großen deutschen Auskunfteien durch. Dabei stellten wir zahlreiche Verstöße gegen das Bundesdatenschutzgesetz fest.

Eine Auskunftei darf nur dann personenbezogene Daten an einen Kunden übermitteln, wenn dieser ein *berechtigtes Interesse* an den gewünschten Daten darlegt (§ 29 Abs. 2 BDSG). Ein berechtigtes Interesse eines Kunden liegt z.B. vor, wenn dieser dem betroffenen Bürger einen Kredit einräumen will oder prüfen möchte, ob es sich lohnt, eine bestehende Forderung bei ihm zu vollstrecken. Bei der Glaubhaftmachung des berechtigten Interesses begnügte sich die Auskunftei damit, daß der Kunde in einem Formular wenig aussagekräftige Anfragegründe, wie etwa „Geschäftsanbahnung" oder „Bonitätsprüfung" ankreuzte. Durch dieses Verfahren erfüllt die Auskunftei nicht die gesetzliche Verpflichtung, sich das berechtigte Interesse des Kunden an der gewünschten Datenübermittlung darstellen zu lassen. Hierfür reichen die gewählten Schlagworte nicht aus. Eine Geschäftsanbahnung ist etwa dann kein Grund für eine Beauskunftung, wenn das Geschäft sofort abgewickelt wird und der Kunde nicht in Vorleistung treten muß. Das Schlagwort „Bonitätsprüfung" erläutert nur den Wunsch des Kunden, stellt aber keine Darlegung des berechtigten Interesses dar.

Wenn die Auskunftei von einem Kunden um Auskunft zu einer bestimmten Person gebeten wurde, wurden häufig außerdem auch *Daten über den Ehegatten* des Betreffenden mitgeteilt. So wird etwa die Auskunft erteilt, daß der Betroffene zwar über eine gute Bonität verfüge, sein Ehegatte aber eine eidesstattliche Versicherung abgegeben habe. Eine derartige Mitübermittlung von Ehegattendaten ist aber nur in ganz engen Grenzen möglich, nämlich dann, wenn die negativen Kreditmerkmale eines Ehegatten sich bei dem anderen auswirken, etwa wenn der eine Ehegatte dem anderen die Verwaltung seines Vermögens überlassen hat oder er für das zur Diskussion stehende Geschäft in Form eines Strohmanns vorgeschoben wurde.

Der Betroffene ist von den Auskunfteien über die erstmalige Übermittlung und die Art der übermittelten Daten zu *benachrichtigen* (§ 33 Abs. 1 Satz 2 BDSG). In den Fällen, in denen (rechtmäßig oder rechtswidrig) Daten über einen Ehegatten übermittelt wurden, verzichtete die Auskunftei auf eine Benachrichtigung des betroffenen Ehegatten. Die Nichtbeachtung der Benachrichtungspflicht stellt eine Ordnungswidrigkeit dar (§ 44 Abs. 1 Nr. 3 BDSG).

Wenn der Kunde einer Auskunftei sein berechtigtes Interesse darlegt, offenbart er zwangsläufig Daten über seinen Schuldner. Dadurch erfährt die Auskunftei z.B., daß gegen den Schuldner zwei und mehr *„Inkassofälle"* anhängig sind. Zu diesen

Inkassofällen können auch unbegründete Mahnbescheide zählen, die nur „weiche" Negativdaten darstellen. Die Auskunftei speicherte solche Inkassofälle als „harte" Negativdaten, setzte sie also mit eidesstattlichen Versicherungen gleich und teilte sie anderen Kunden auf Anfrage mit. Dies verstößt gegen § 29 BDSG.

Auskunfteien sind verpflichtet, die personenbezogenen Daten der Betroffenen *zu löschen*, wenn eine Prüfung am Ende des 5. Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist (§ 35 Abs. 2 Nr. 4 BDSG). Die Auskunftei löschte zwar nach Ablauf dieses Zeitraumes die Bonitätsdaten, speicherte aber weiterhin Name und Anschrift des Betroffenen. Da das Bundesdatenschutzgesetz eine vollständige Löschung der nicht mehr benötigten Daten vorsieht, ist die weitere Speicherung eines Rumpfdatensatzes rechtswidrig.

Datenübermittlungen *an Kunden im Ausland* erfolgten in dem gleichen Umfang und unter den gleichen Bedingungen wie bei inländischen Kunden. Wir haben dem Unternehmen empfohlen, dieses Verfahren nur dann beizubehalten, wenn der Kunde seinen Sitz in einem EU-Land oder einem Nicht-EU-Land mit ausreichendem Datenschutzniveau (z.B. Norwegen, Schweiz) hat. Bei einer Datenübermittlung in ein Land ohne ausreichendes Datenschutzniveau (z.B. Polen, Singapur, Indien) sollte sich der ausländische Kunde zumindest gegenüber dem Unternehmen vertraglich zur kontrollierbaren Einhaltung der wesentlichen deutschen Datenschutzbestimmungen verpflichten (Art. 26 EU-Datenschutzrichtlinie)[120].

SCHUFA

Die SCHUFA – Schutzgemeinschaft für allgemeine Kreditsicherung – ist eine Gemeinschaftseinrichtung der kreditgebenden deutschen Wirtschaft. Die vertragliche Verpflichtung der SCHUFA, Auskünfte zu erteilen, steht der Verpflichtung der Vertragspartner gegenüber, der SCHUFA Informationen über den Datenbestand zur Verfügung zu stellen.

Das Verfahren stellt grundsätzlich auch sicher, daß alle positiven Daten über einen Betroffenen, etwa die Erfüllung einer Forderung, rechtzeitig gespeichert werden, damit sie bei der Entscheidung über eine Kreditvergabe berücksichtigt werden können.

Der Grundsatz, daß auch alle Positivdaten über einen Betroffenen eingemeldet werden, wird unterbrochen, wenn der Vertragspartner die Forderung gegen den Betroffenen an einen Nichtvertragspartner der SCHUFA verkauft. Bei der SCHUFA erhält der Betroffene dann das Merkmal „VF" *(Verkauf der Forderung)*. Der Nichtvertragspartner der SCHUFA hat nicht die Verpflichtung, die möglicherweise kurz nach dem Forderungsverkauf erfolgte Erfüllung der Forderung bei der SCHUFA zurückzumelden. Der Bankkunde kann froh sein, wenn er von einem Vertragspartner der SCHUFA, der eine entsprechende Auskunft („VF") bei der SCHUFA eingeholt hat, wenigstens die Gelegenheit erhält, über den Verbleib der Forderung Auskunft zu erhalten. In vielen Fällen werden aber die über das Merkmal „VF" informierten SCHUFA-Vertragspartner davon Abstand nehmen, mit einem durch dieses Merkmal belasteten Bürger einen Vertrag abzuschließen, ohne daß der betroffene Bürger je von dem Grund des Nichtabschlusses des Vertrages oder ähnlicher negativer Folgen Kenntnis erhält, so geschehen im Fall einer Petentin, die ein Handy erwerben wollte.

[120] vgl. 1.1

Wir haben der SCHUFA empfohlen, die oben dargestellten negativen Folgen des Merkmals „VF" zu verhindern. Wir empfahlen, daß die SCHUFA ihre Vertragspartner verpflichtet, sie oder die SCHUFA direkt über das Schicksal der abgetretenen Forderung zu informieren. Die Informationspflicht sollte mit einer Vertragsstrafenklausel abgesichert werden. Die SCHUFA ist unserem Vorschlag bisher leider nicht gefolgt.

Schwarze Schafe

Wir berichteten über drei Berliner Auskunfteien, die in dem Verdacht stehen, illegal personenbezogene Daten erhoben zu haben[121]. Das 1995 eingeleitete *Strafverfahren* ist bisher noch nicht abgeschlossen. Nach der Veröffentlichung der Vorwürfe kündigten fast alle Kunden ihre Verträge. Wegen der aufgetretenen wirtschaftlichen Probleme beantragten die Geschäftsführer die Eröffnung eines Konkursverfahrens, welches mangels Masse abgelehnt wurde. Die Unternehmen gingen daraufhin in Liquidation. Während der Liquidationsphase untersuchten wir die Geschäftsräume. Wir überzeugten uns davon, daß die liquidierten Unternehmen ihre Arbeit eingestellt hatten.

Zwar versuchten einige Geschäftsführer und Mitarbeiter der liquidierten Unternehmen, zwei neue Auskunfteien aufzubauen.

Es gelang ihnen jedoch nicht mehr, Kunden zu akquirieren, so daß die Unternehmen nach wenigen Wochen aufgaben. Insbesondere bei einem der Nachfolgeunternehmen war offensichtlich, daß die Inhaber beabsichtigten, weiterhin rechtswidrig Daten zu erheben. In einem Werbeschreiben hatten sie anderen Detekteien und Auskunfteien die Ermittlung geheimer Telefonnummern angeboten.

[121] JB 1995, 6.3

4.6.3 Allerlei Gewerbe

Aktenvernichtung

Auf einem frei zugänglichen Pritschenwagen fanden sich die Akten einer Anwaltskanzlei. Einige dieser Akten enthielten sehr sensible Daten (Strafverfahren wegen sexuellen Mißbrauchs von Minderjährigen). Ein Bürger beobachtete, daß Kinder mit den Akten spielten, und schaltete uns ein. Er berichtete uns, daß er einige Tage vorher auf dem Pritschenwagen Daten eines Steuerberaters vorgefunden habe. Der Pritschenwagen gehörte einem Altpapierverwerter.

In vielen Unternehmen, bei Steuerberatern und sogar bei Rechtsanwälten besteht Unklarheit darüber, wie größere Aktenmengen datenschutzgerecht vernichtet werden können. Die Einschaltung eines Aktenvernichtungsunternehmens ist zwar kostengünstiger als etwa die Anschaffung eines eigenen geeigneten Aktenvernichters, unterliegt aber einigen Voraussetzungen, auf die oft nicht geachtet wird. So muß dieser in dem nach § 32 BDSG von der Aufsichtsbehörde geführten Register eingetragen sein. Die speichernde Stelle trägt die volle Verantwortung für die bis zur Vernichtung zu beachtenden technischen und organisatorischen Maßnahmen. Demgegenüber gehen viele Unternehmen zu Unrecht davon aus, daß sie mit der Abgabe ihrer Akten an einen gewerblichen Aktenvernichter auch die Verantwortung für eine datenschutzgerechte Vernichtung abgegeben haben.

Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung und der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§ 11 Abs. 2 BDSG). Zwingend vorgeschrieben ist auch, daß der Auftrag *schriftlich* zu erteilen ist, wobei die Art der Datenverarbeitung oder Nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Die Vorgaben an den Auftragsdatenverarbeiter müssen so detailliert sein, daß sie nötigenfalls gerichtlich durchgesetzt werden können. Insbesondere sollte geregelt werden[122],

- um welche Art von Datenträgern und Daten es sich handelt (z.B. Rechnungen, Personalunterlagen) und wie die Schutzbedürftigkeit der Daten einzustufen ist;
- auf welche Weise die Vernichtung unter Berücksichtigung der Schutzbedürftigkeit der Daten zu erfolgen hat (bei Datenträgern in Papierform ist in jedem Fall die Papierstreifenbreite bzw. Partikelgröße der Vernichtung zu vereinbaren; bei der Löschung und Entsorgung elektronischer/magnetischer Speichermedien sind die näheren Einzelheiten festzulegen);
- wo die Vernichtung durchgeführt wird (vor Ort beim Auftraggeber, in der Betriebsstätte des Auftragnehmers oder bei einem Subunternehmer);
- von wem die Datenträger abgeholt werden (Auftragnehmer oder beauftragte Speditionsfirma) und auf welche Weise sie transportiert werden (z.B. in verschlossenen Behältnissen);
- wie die Datenträger bis zur Vernichtung aufzubewahren sind (etwa in verschlossenen Räumen oder Containern) und wann sie zu vernichten sind (am Tag der Abholung oder innerhalb welchen Zeitraums);
- daß die Verfügungsbefugnis des Auftraggebers bis zum Abschluß der Vernichtung weiterbesteht;
- ob und welche Unterauftragnehmer der Auftragnehmer zur Erfüllung seiner Vertragspflichten einschalten darf und die Verpflichtung, im Vertrag zwischen dem Auftragnehmer und

[122] Amtliche Mitteilung, Staatsanzeiger des Landes Baden-Württemberg vom 9. Januar 1993

Subunternehmern sicherzustellen, daß sich diese der Kontrolle des Auftraggebers und des Auftragnehmers unterwerfen;
– daß der Auftraggeber berechtigt ist, den Transport, die Aufbewahrung und die Vernichtung der Datenträger vor Ort zu überwachen (bei wiederholter oder ständiger Überlassung von Vernichtungsgut genügt es, wenn eine solche Überwachung stichprobenweise erfolgt);
– daß der Auftragnehmer zur Abgabe einer schriftlichen Vernichtungsbescheinigung verpflichtet ist, aus der sich ergibt, wann welche Unterlagen auf welche Weise vernichtet worden sind.

Unternehmen, die Akten vernichten lassen wollen, die einer besonderen Geheimhaltungspflicht unterliegen (Akten aus Krankenhäusern, Anwalts- und Steuerpraxen etc.) empfehlen wir im übrigen, neben den schon dargestellten Vorgaben immer eine Person abzustellen, die die Datenträger bis zur Vernichtung „begleitet".

Im vorliegenden Fall haben sich der Rechtsanwalt und der Steuerberater mit einem Vernichtungsprotokoll des Altpapierverwerters begnügt. Eine weitergehende Überprüfung der Aktenvernichtung fand nicht statt – diese war nach der Behauptung des Altpapierverwerters nicht einmal Vertragsbestandteil. Da datenschutzgerecht vernichtetes Material sich als Altpapier nicht mehr verwerten läßt, ist die Beauftragung eines bloßen Altpapierverwerters (im Gegensatz zu einem Aktenvernichtungsunternehmen) zwar in aller Regel kostengünstiger, sie genügt aber in keinem Fall den gesetzlichen Bestimmungen.

Private Register

Ein Berliner Unternehmen ermittelt bundesweit aus Telefonbüchern, Adreßverzeichnissen sowie mit Hilfe der CD-ROM-Fassung der Telefonbücher die Namen sowie die Anschriften von Handwerkern und Gewerbetreibenden. Die erhobenen Daten werden dazu benutzt, den Betroffenen eine „Offerte zur Registrierung der Deutschen Handwerksbetriebe" bzw. eine „Offerte zur Registrierung der Deutschen Gewerbebetriebe" zu machen. Der Angeschriebene wird in das Register aufgenommen, wenn er einen bestimmten Geldbetrag überweist. Die Offerte enthält den Hinweis, daß die Daten zur Auskunft an die im Register eingetragenen Firmen und sonstige bestimmt sind.

Mehrere der von dem Unternehmen verwendeten Formulare wurden inzwischen vom Landgericht Berlin verboten, da sie bei flüchtiger Betrachtung den Anschein erweckten, es handele sich bei dem „Handwerksregister" um ein amtliches Register oder zumindest um ein Register der Handwerksorganisationen. Die Datenerhebung, die Nutzung (Anschreiben an die Betroffenen) und die Speicherung der personenbezogenen Daten von Betroffenen mit dem Ziel, ihre Daten unter Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb (nach §§ 1, 3 Gesetz gegen den unlauteren Wettbewerb sind irreführende Angaben untersagt) in ein Register aufzunehmen, sind rechtswidrig, da eine rechtmäßige Datenverarbeitung und Nutzung nur dann vorliegen kann, wenn bei dem Datenfluß keine sonstigen Rechtsvorschriften verletzt sind.

Visitenkartenautomat

Die Software eines Visitenkartenautomaten enthielt einen folgenschweren Fehler. Anstatt der versprochenen 25 Visitenkarten erhielt der Kunde nur 24 Karten. Außerdem erhielt er eine Visitenkarte des vorherigen Kunden. Da die Mehrzahl der Kunden die Visitenkarte des Vorkunden zurücklegte, befanden sich nach kurzer Zeit zahlreiche

Visitenkarten der jeweiligen Vornutzer im Automaten.

Als wir den Automatenbesitzer auf den Computerfehler aufmerksam machten, teilte uns dieser mit, daß er den Fehler inzwischen behoben habe. Eine Vor-Ort-Überprüfung ergab allerdings, daß der Fehler nicht behoben worden war. Offenbar hatte der Besitzer uns die Unwahrheit gesagt, um einen finanziellen Verlust durch die Stillegung des Visitenkartenautomaten zu verhindern. Nach längerer Diskussion war der Automatenbesitzer bereit, den Automaten bis zu seiner Reparatur stillzulegen.

4.7 Telekommunikation und Medien

4.7.1 Entwicklung des Telekommunikationsrechts

Das Telekommunikationsgesetz (TKG)[123], das die letzte Stufe der Liberalisierung im Telekommunikationsbereich („Postreform III“) bildet, ist im Berichtszeitraum in Kraft getreten[124].

Das Telekommunikationsgesetz enthält jetzt auch Regelungen zum Datenschutz, die vorher nur auf der Ebene von Rechtsverordnungen (Telekom-Datenschutzverordnung – TDSV bzw. Teledienstunternehmen-Datenschutzverordnung – UDSV) festgelegt waren. Entgegen den ursprünglichen Entwürfen ist die Wahrung des *Fernmeldegeheimnisses* ausdrücklich als Regulierungsziel in das Gesetz aufgenommen worden (§ 2 Abs. 2 Nr. 1 TKG). Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, dürfen personenbezogene Daten ihrer Kunden, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, für Zwecke der *Werbung, Kundenberatung oder Marktforschung* nur noch dann nutzen, wenn der Kunde eingewilligt hat. Die Eintragung in öffentliche *gedruckte oder elektronische Verzeichnisse* erfolgt nur, soweit der Kunde dies beantragt hat. Die Betroffenen können bestimmen, ob und welche Angaben in den Kundenverzeichnissen veröffentlicht werden sollen. Zusätzlich ist den Kunden endlich das bereits mehrfach in vergangenen Berichtsjahren geforderte, nach Medien differenzierte Wahlrecht zur Veröffentlichung ihrer Daten in Kundenverzeichnissen eingeräumt worden. Damit ist es möglich, die entsprechenden Angaben zwar in gedruckten, nicht aber in elektronischen Verzeichnissen veröffentlichen zu lassen (§ 89 Abs. 8 TKG).

Bei anderen Problemen konnten keine befriedigenden Lösungen erreicht werden. So ist der § 12 des Fernmeldeanlagengesetzes, der zur Erteilung von Auskünften „über die Telekommunikation“ an *Gerichte und Staatsanwaltschaften* im Rahmen beliebiger strafgerichtlicher Untersuchungen verpflichtet, entgegen der wiederholten Forderung der Konferenz der Datenschutzbeauftragten[125] weder gestrichen noch in verfassungskonformer Weise geändert worden.

Neu ist auch eine Vorschrift, die Anbieter von Telekommunikationsdiensten zur Führung von Kundendateien verpflichtet, für die der Regulierungsbehörde für Zwecke der Gerichte und Staatsanwaltschaften, der Polizei, der Zollbehörden sowie der Nachrichtendienste ein automatisiertes Abrufverfahren ermöglicht werden soll (§ 90 TKG). Die Diensteanbieter müssen sicherstellen, daß ihnen Abrufe durch die berechtigten Stellen nicht zur Kenntnis gelangen. Wir hatten im Rahmen des Gesetzgebungsverfahrens insbesondere kritisiert, daß der Zugriff auf

[123] BGBl. I, S. 1120
[124] vgl. JB 1995, 4.3
[125] vgl. zuletzt JB 1994, 5.1, Anlage 2.5

die Kundendaten für die genannten Stellen zur Erfüllung ihrer gesetzlichen Aufgaben nahezu schrankenlos zulässig ist, und eine stärkere Bindung an die Verfolgung konkreter Straftaten gefordert. Dieser Empfehlung ist der Gesetzgeber nicht gefolgt.

Dieses Verfahren schafft eine Infrastruktur, die datenschutzpolitisch das Telekommunikationsnetz in die Nähe eines Fahndungsnetzes für diese Behörden rückt. Damit verändert sich die Funktion dieses zentralen Kommunikationsnetzes, das in seiner bisherigen (analogen) Form technisch zur Fahndung nur bedingt geeignet war. Der Zweckentfremdung sind keine technischen, sondern nur noch rechtliche Schranken gesetzt. Zudem sind die Diensteanbieter, die den Zugriff der Sicherheitsbehörden auf ihre Kundendateien nicht registrieren dürfen, nicht in der Lage, die befugten Zugriffe dieser Stellen von unbefugten Zugriffen zu unterscheiden. Dies widerspricht allen bisher in anderen Rechtsbereichen vorgesehenen Sicherheitsvorkehrungen und Kontrollpflichten der datenverarbeitenden Stellen beim Online-Zugriff von außen.

Weitere Kundendaten sollen darüber hinaus im Einzelfall für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste oder des Zollkriminalamtes den zuständigen Stellen übermittelt werden (§ 89 Abs. 6 TKG). Auskünfte an die genannten Stellen dürfen auch hierbei Kunden oder Dritten nicht mitgeteilt werden. Die Möglichkeiten zur Erhebung personenbezogener Daten bei Diensteanbietern sind damit gegenüber der vorher gültigen Bestimmung des § 10 Abs. 4 Nr. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) nochmals erweitert worden. Zumindest das Verbot der Information des Kunden über die Einzelauskunft ist verfassungsrechtlich problematisch.

Die Vorschriften über die Kontrolle des Datenschutzes wurden insofern verändert, als nunmehr der Bundesbeauftragte für den Datenschutz als zentrale Stelle für die Kontrolle der Einhaltung von Datenschutzbestimmungen bei Unternehmen, die in den Geltungsbereich des TKG fallen, zuständig ist – für Sprachtelephonie allerdings erst ab 1. Januar 1998 (§ 91 Abs. 4 TKG). Für das Angebot von Telekommunikationsdienstleistungen durch öffentliche Stellen der Länder bleiben jedoch auch darüber hinaus weiterhin die Landesbeauftragten für den Datenschutz zuständig.

Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV)

Noch auf der Grundlage des Post- und Telekommunikationsregulierungsgesetzes ist am 19. Juli 1996 die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) in Kraft getreten[126]. Die Verordnung ersetzt die bis dahin für die Deutsche Telekom AG gültige Telekom-Datenschutzverordnung und die Teledienstunternehmen-Datenschutzverordnung (UDSV), die für private Wettbewerber der Telekom galt. Sie enthält einige wesentliche Änderungen der bisherigen Rechtslage.

Im Regelfall ist ein Telekommunikationsunternehmen nur dazu berechtigt, die *Zielnummer* nach dem Ende der Verbindung um die letzten drei Ziffern *gekürzt* zu speichern. Etwas anderes gilt nur, wenn der Kunde sich entweder für eine vollständige Löschung oder vollständige Speicherung entscheidet. Die Deutsche Telekom AG setzt sich über diese eindeutige Rechtslage allerdings bei Auslandsgesprächen mit dem bemerkenswerten Argument hinweg, die Verordnung sei technisch überholt, und speichert hier im Regelfall vollständige Zielnummern.

[126] BGBl. I, S. 982

Im Gegensatz zur gegenwärtigen Praxis der Deutschen Telekom AG können nunmehr nach Wahl des anrufenden Kunden *Einzelverbindungsnachweise* mit vollständigen Zielnummern erstellt werden, ohne daß der angerufene Kunde der Aufnahme seiner Zielnummer in die Einzelentgeltnachweise widersprechen kann (§ 6 Abs. 7 TDSV). Die Einführung einer solchen Wahlmöglichkeit für den Angerufenen, wie sie in den Niederlanden bereits praktiziert wird, hatten wir empfohlen. Durch dieses Verfahren hätte auch die Problematik der Aufnahme von Anrufen bei telefonischen Beratungsstellen in Einzelverbindungsnachweise unbürokratisch gelöst werden können. Bis zum Ende des Berichtszeitraums hat die Telekom auf die Erstellung von Einzelentgeltnachweisen mit vollständigen Zielnummern verzichtet.

Für die Eintragung in öffentliche Kundenverzeichnisse räumt die neue TDSV in Übereinstimmung mit dem TKG den Kunden ein differenziertes *Wahlrecht* ein. Damit können die Kunden erstmals zwar in gedruckten Teilnehmerverzeichnissen eingetragen sein, gleichzeitig aber die Aufnahme ihrer Daten in elektronische Teilnehmerverzeichnisse ausschließen. Diese Einträge sind in den gedruckten Kundenverzeichnissen gesondert zu kennzeichnen. Dadurch sollen auch Informationsanbieter, die nicht in den Geltungsbereich der TDSV fallen und lediglich elektronische Teilnehmerverzeichnisse – z.B. auf CD-ROM – anbieten, darauf hingewiesen werden, daß der Kunde eine Aufnahme seiner Daten in elektronische Kundenverzeichnisse nicht wünscht.

Der Verordnungsgeber hat nunmehr unmißverständlich klargestellt, daß das Angebot zur *Unterdrückung der Anzeige der Rufnummer des Anrufers* beim angerufenen Anschluß kostenfrei erfolgen muß (§ 9 Abs. 1 TDSV). Für dieses Leistungsmerkmal hatte die Deutsche Telekom AG in der Vergangenheit Gebühren erhoben.

Bei der Rufnummernauskunft sind grundlegende Änderungen eingetreten: Die Weitergabe der Rufnummer durch den Telefonauskunftsdienst ist nach Wahl des Kunden auch dann möglich, wenn er der Aufnahme seiner Daten in Teilnehmerverzeichnisse widersprochen hat. Dies war in der Vergangenheit von verschiedenen Fernmeldeämtern in der Bundesrepublik unterschiedlich gehandhabt worden.

Zukünftig können auch über die Rufnummer hinausgehende Auskünfte über in Teilnehmerverzeichnissen veröffentlichte Kundendaten gegeben werden. Während dies für Neukunden nur aufgrund ihrer Einwilligung erfolgen darf, hat der Verordnungsgeber für Kunden, mit denen zum Zeitpunkt des Inkrafttretens bereits ein Vertragsverhältnis besteht, eine Widerspruchslösung vorgesehen.

Die TDSV war bereits zum Zeitpunkt ihres Inkrafttretens wieder novellierungsbedürftig, da sie an die neue Verordnungsermächtigung des TKG angepaßt werden muß.

Multimedia-Gesetzgebung in Bund und Ländern

Mit dem schrittweisen Inkrafttreten des Telekommunikationsgesetzes werden die rechtlichen Rahmenbedingungen für Betreiber von Telekommunikationsnetzen festgelegt. Ungeregelt ist dagegen bisher die *Nutzung* dieser Netze, wenn man vom Sprachtelefondienst absieht. Der *Bildschirmtext-Staatsvertrag*, der seit 1983 eine bestimmte Form der Nutzung des bundesweiten Telefonnetzes außerhalb des Sprachtelefondiensts regelte,

muß weitgehend als technisch überholt angesehen werden. Insbesondere bereitet seine Anwendung auf Online-Dienste erhebliche Schwierigkeiten. Auch der *Rundfunkstaatsvertrag Berlin-Brandenburg von 1992*[127] regelt zwar die Erprobung von rundfunkähnlichen sonstigen Diensten durch Nutzung neuer Techniken oder neuer Nutzungsformen (§ 47) im Anschluß an das Kabelpilotprojektgesetz von 1984. Auch diese Regelungen erfassen jedoch die *neuen Tele- und Mediendienste* nur unzureichend.

Die Datenschutzbeauftragten haben sich seit Anfang der 80er Jahre für eine datenschutzgerechte Regelung der Verarbeitung von Verbindungs- und Abrechnungsdaten nicht nur auf der Ebene der Netze, sondern auch auf der Nutzungsebene eingesetzt. Speziell Berlin hat seit dem Kabelpilotprojektgesetz von 1984 in diesem Bereich stets eine Vorreiterrolle eingenommen. Bei der jetzt anstehenden Schaffung eines neuen Regelungsrahmens für Tele- und Mediendienste, die nicht als Rundfunk im herkömmlichen Sinne zu bezeichnen sind, wird es darauf ankommen, das bisherige Schutzniveau für den Bürger beizubehalten und – soweit neue Risiken erkennbar werden – zu verbessern.

Die Datenschutzbeauftragten haben darüber hinaus in einer Entschließung zu *Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten* vom 29. April 1996[128] betont, daß Dienste und Multimedia-Einrichtungen so gestaltet werden müssen, daß keine oder möglichst wenige personenbezogenen Daten erhoben, verarbeitet und genutzt werden; deshalb seien auch anonyme Nutzungs- und Zahlungsformen anzubieten. Dieser Entschließung waren mehrere Anhörungen in München und Hamburg vorausgegangen, bei denen sich die Datenschutzbeauftragten von Vertretern der Online-Dienste deren Sichtweise erläutern ließen. Der *Grundsatz der Datensparsamkeit bzw. Datenarmut* war bereits im *Bericht des Rates für Forschung, Technologie und Innovation zur Informationsgesellschaft* vom Dezember 1995[129] als Element eines modernen Datenschutzrechts gekennzeichnet worden. Nachdem der lange schwelende Streit zwischen Bund und Ländern über die Frage der Regelungskompetenz im Multimedia-Bereich Anfang Juli 1996 zumindest vorläufig beigelegt worden war, begannen Abstimmungsgespräche zwischen Bund und Ländern mit dem Ziel, zu möglichst einheitlichen Regelungen auf Bundes- und Landesebene für alle neuen Multimedia-Dienste zu gelangen. An diesen Gesprächen haben wir uns intensiv beteiligt. Der am 11. Dezember 1996 vom Bundeskabinett beschlossene Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (*Informations- und Kommunikationsdienste-Gesetz*)[130] und der wenig später von den Ministerpräsidenten der Länder gebilligte Entwurf eines Mediendienste-Staatsvertrags der Länder enthalten in ihren datenschutzrechtlichen Teilen weitgehend identische Vorschriften. Artikel 2 des Entwurfs für ein IuK-Dienste-Gesetz des Bundes beschäftigt sich ausschließlich mit dem Datenschutz bei Telediensten (Teledienstedatenschutzgesetz); demgegenüber finden sich die Datenschutzbestimmungen auf Länderseite im III. Abschnitt des Mediendienste-Staatsvertragsentwurfs.

Die jeweiligen Geltungsbereiche der bundes- und landesrechtlichen Regelungen sollen in der Weise voneinander abgegrenzt

[127] Staatsvertrag über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks vom 29. Februar 1992, GVBl. S. 150

[128] Anlage 2.4

[129] Informationsgesellschaft, Chancen, Innovationen und Herausforderungen (Feststellungen und Empfehlungen), S.31

[130] BR-Drs. 966/96

werden, daß der Bund Regelungen für Angebote im Bereich der *Individualkommunikation* (Teledienste, z.B. Telebanking, Datenaustausch, Angebote zur Nutzung des Internets oder weiterer Netze, Telespiele) trifft, während die Länder das Angebot und die Nutzung von *an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten (Mediendiensten)* regeln. Im einzelnen werden sich in der Praxis voraussichtlich Schwierigkeiten bei der Frage ergeben, ob Bundes- oder Landesrecht anwendbar ist.

Positiv hervorzuheben an beiden Entwürfen ist vor allem die Verpflichtung des Diensteanbieters, den Nutzern die Inanspruchnahme von Tele- und Mediendiensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Damit wird eine zentrale Forderung der Datenschutzbeauftragten aufgegriffen, die stets eine Option für den Bürger zur spurlosen Nutzung von Multimedia-Diensten gefordert hatten. Erstmals findet damit das Gebot der Datenvermeidung jedenfalls in Form einer zwingend vorgeschriebenen Nutzungsvariante Eingang in die deutsche Gesetzgebung (vgl. auch oben 2.2).

Positiv zu bewerten ist auch, daß der Diensteanbieter Daten über den Nutzer nur in transparenter Weise erheben darf. Dies gilt auch für die Verwendung sogenannter *Cookies* („Kekse"), die von Diensteanbietern im Multimedia-Bereich zunehmend eingesetzt werden[131].

Der Entwurf des Mediendienste-Staatsvertrags sieht die Einführung des *„Datenschutz-Audit"* vor. Dabei handelt es sich um ein Gütesiegel („Blauer Engel" für datenschutzfreundliche Gestaltung eines Angebots), das nach dem Vorbild des Umwelt-Audits[132] von zugelassenen Gutachtern vergeben werden soll. Die Einführung eines solchen Datenschutz-Audits wäre eine wichtige Ergänzung der bisherigen Möglichkeiten zur Durchsetzung und Verbesserung des Datenschutzes (auch außerhalb des Multimedia-Bereichs). Ein solches Gütesiegel könnte von den Anbietern dazu benutzt werden, um auf dem Markt Wettbewerbsvorteile durch datenschutzfreundliche Dienstleistungen zu erlangen. Dabei geht es keineswegs nur um die Einhaltung der datenschutzrechtlichen Verpflichtungen im engeren Sinn, die ohnehin bestehen. Vielmehr könnte „Datenschutz" auch zum Verkaufsargument in der Weise werden, daß ein Anbieter sich von einem unabhängigen Gutachter bescheinigen läßt, daß er über die gesetzlichen Verpflichtungen zugunsten des Nutzers hinausgeht. In diesem Zusammenhang hätte das Datenschutz-Audit auch eine wichtige Funktion bei der *Sicherstellung eines hohen Datenschutzstandards im internationalen Bereich*. Da Aufsichtsmaßnahmen (Untersagungsverfügungen o.ä.) gegen ausländische Anbieter ohnehin nicht verhängt werden können, kommt es darauf an, im Inland die Datenschutzfreundlichkeit eines Multimedia-Angebots verkaufsfördernd einzusetzen, so daß auch ausländische Anbieter, die in Deutschland Kunden werben wollen, gehalten sind, sich um ein entsprechendes Gütesiegel zu bemühen.

Deshalb ist es unverständlich, weshalb die Bundesregierung eine Vorschrift, die das Datenschutz-Audit auch im Bereich der Teledienste in früheren Entwürfen des IuK-Dienste-Gesetzes vorsah, gestrichen hat. In diesem Punkt haben wir uns für eine Wiederaufnahme des Datenschutz-Audits in den Bundesentwurf eingesetzt, auch um ein Auseinanderfallen der rechtlichen Stan-

[131] vgl. unten 4.8.4

[132] vgl. Gesetz zur Ausführung der Verordnung (EWG) Nr.1836/93 des Rates vom 29. Juni 1993 über die freiwillige Beteiligung gewerblicher Unternehmen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung (Umwelt-Auditgesetz – UAG) BGBl. 1995, 1591

dards in diesem Bereich zu verhindern.

Noch in einem weiteren Punkt weichen der Gesetzentwurf der Bundesregierung und der Staatsvertragsentwurf der Länder voneinander ab:

Entsprechend dem TKG will die Bundesregierung Diensteanbieter dazu verpflichten, Bestandsdaten auf Ersuchen an die zuständigen Stellen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Gefahrenabwehr oder für die Erfüllung der Aufgaben der Nachrichtendienste und des Zollkriminalamtes zu übermitteln. Die Folgen wären hier noch gravierender als im Netzbereich. Jeder Anbieter eines Homebanking-Dienstes wäre z.B. verpflichtet, der Polizei oder den Verwaltungsbehörden ohne weitere Voraussetzungen (auch zur Verfolgung von Ordnungswidrigkeiten) Auskunft über seine Kunden zu geben. Interne Schutzregelungen der Banken und Sparkassen zum „Bankgeheimnis“ der Kunden würden damit unterlaufen. Über die bisherige Rechtslage hinaus würde auch den Nachrichtendiensten ein privater Datenbestand offenstehen. Eine andere Folge dieser Regelung wäre, daß Anbieter von elektronischen Informationsdiensten (z.B. Online-Zeitungen), soweit sie in den Anwendungsbereich des IUK-Dienste-Gesetzes fallen, offenlegen müßten, welche ihrer Kunden welche Dienste z.B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff in die Informations- und Meinungsfreiheit des Einzelnen. Die Digitalisierung des Informationsabrufs würde einhergehen mit einer stärkeren Überwachbarkeit des Nutzerverhaltens.

Eine derartige *„Verpolizeilichung“ des Marktes für Teledienste* ist strikt abzulehnen. In keinem anderen Wirtschaftsbereich und erst recht nicht im bisher geltenden Medienrecht sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt. Das geltende Strafprozeßrecht und die Polizeigesetze der Länder enthalten insoweit ausreichende Befugnisse zur Verbrechensbekämpfung auch im Bereich der Multimedia-Dienste. Ein Bedarf zur Übermittlung derartiger Daten an die Nachrichtendienste ist ohnehin nicht erkennbar.

Die Länder haben daher zu Recht die Übernahme einer entsprechenden Regelung in den Entwurf eines Staatsvertrages über Mediendienste abgelehnt. Wir haben uns dafür eingesetzt, daß auch der Gesetzentwurf der Bundesregierung auf diese pauschale Überwachungsklausel verzichtet.

Übrigens setzt sich die Tendenz zur Sicherstellung der Überwachbarkeit von Telekommunikation auch im *Entwurf des Signaturgesetzes* (Artikel 3 des IuK-Dienste-Gesetzes) fort. Zwar eröffnet dieser Gesetzentwurf dem Einzelnen, der ein Zertifikat für eine *digitale Signatur* bei der Zertifizierungsstelle beantragt, auf dem Zertifikat entweder seinen wirklichen Namen oder ein Pseudonym eintragen zu lassen. Damit erkennt die Bundesregierung an, daß ein legitimes Interesse des Einzelnen darin bestehen kann, auch bei der Verwendung elektronischer Unterschriften seine Identität nicht preiszugeben. Andererseits soll die Zertifizierungsstelle verpflichtet werden, bei einem Signaturschlüssel-Inhaber mit *Pseudonym* die Daten über dessen Identität an die genannten Sicherheitsbehörden zu übermitteln. Es ist nicht erkennbar, weshalb ein Bürger, der ein Zertifikat für eine *elektronische Unterschrift* mit Pseudonym erhalten hat, damit rechnen muß, daß seine Identität auch von den Verfassungsschutzbehörden und den Nachrichtendiensten ermittelt werden kann. Die an sich begrüßenswerte Option für den Schlüsselinhaber, ein Pseudonym zu wählen, wird durch den *pauschalen Identifikationsvorbehalt der Sicherheitsbehörden* praktisch entwertet. Auch wenn die Behörden durch die geplante Regelung nicht etwa ermächtigt

werden, digitale Unterschriften ihrerseits zu verfälschen, was die Beweiskraft jeder elektronischen Signatur in Frage stellen würde, ist die geplante Regelung zur Aufhebung eines Pseudonyms doch geeignet, das wichtige Vertrauen in die aufzubauende Sicherheitsinfrastruktur zu erschüttern.

Sobald der Staatsvertrag und das IuK-Dienste-Gesetz in Kraft treten, wird viel von einer effektiven *Kontrolle und Durchsetzung der datenschutzrechtlichen Vorschriften* abhängen. Vor allem darf es nicht zu einer unterschiedlichen Auslegung der neuen Rahmenbedingungen in den einzelnen Bundesländern kommen.

Die Bundesregierung hat es zwar bei der Kontrollstruktur des Bundesdatenschutzgesetzes und damit der Zuständigkeit der Aufsichtsbehörden auch im Bereich der Teledienste belassen. Die Zuständigkeiten der Landesbeauftragten für den Datenschutz und der Rundfunkdatenschutzbeauftragten bleiben ohnehin unberührt. Allerdings werden die Länder dafür Sorge tragen müssen, daß die Datenschutzaufsicht effektiv koordiniert wird. Wir haben deshalb bereits vor dem Gesetzesbeschluß der Bundesregierung mehrere Gespräche mit den Datenschutzbeauftragten des Bundes und der Länder, den Obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich und den Rundfunkdatenschutzbeauftragten geführt, um eine solche effektive Koordinierung zu erreichen. Die Gespräche werden fortgesetzt. Die Bundesregierung hat angedeutet, daß sie einen erneuten Prüfungsbedarf zur Frage der einheitlichen Datenschutzkontrolle im Bereich der Teledienste sieht, wenn es bis zum Abschluß des Gesetzgebungsverfahrens für das IuK-Dienste-Gesetz nicht gelingt, auf Länderseite zu einer praktikablen und effektiven Koordinierung zu kommen.

Telekommunikationsdatenschutz in Europa kommt voran

Auf europäischer Ebene wurden 1996 entscheidende Fortschritte bei der Beratung des lange verzögerten Entwurfs für eine *ISDN-Richtlinie*[133] gemacht. Es ist vor allem das Verdienst der italienischen Ratspräsidentschaft, daß der Europäische Rat sich im Juni 1996 politisch auf einen Gemeinsamen Standpunkt zu diesem Richtlinienentwurf verständigte, der am 12. September 1996 formell beschlossen wurde[134].

Der Richtlinienentwurf in der Fassung des Gemeinsamen Standpunkts hat einen weitergehenden Anwendungsbereich als frühere Entwürfe. Er soll nicht mehr auf digitale Telekommunikationsnetze beschränkt sein, sondern die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation allgemein regeln. Die Bundesregierung konnte sich im Rat mit ihrem Vorschlag nicht durchsetzen, den Anwendungsbereich der Richtlinie auf *unternehmensinterne Netze (Corporate Networks)* auszudehnen. Allerdings bestand Einigkeit im Rat darüber, daß die Mitgliedstaaten durch die ISDN-Richtlinie nicht daran gehindert werden, die Bestimmungen entsprechend anzuwenden. Im übrigen gilt für unternehmensinterne Netze in jedem Fall die allgemeine Datenschutzrichtlinie. Dies ist deshalb von Bedeutung, weil die Datenschutzbestimmung im deutschen Telekommunikationsgesetz nicht auf öffentlich zugängliche Telekommunikationsdienste beschränkt ist, sondern für alle Unternehmen gilt, die geschäftsmäßig Telekommunikationsdienste erbringen.

Was die *Netzsicherheit* betrifft, so enthält der Gemeinsame Standpunkt nicht mehr wie die Vorentwürfe eine Verpflichtung zum *Angebot von Verschlüsselungsmöglichkeiten*, wenn

[133] vgl. zuletzt JB 1995, 4.4
[134] Gemeinsamer Standpunkt (EG) Nr. 57/96, ABlEG C 315/30

besondere Risiken der Verletzung der Netzsicherheit gegeben sind. In diesem Punkt haben sich offenbar diejenigen Mitgliedstaaten im Rat durchgesetzt, die jede Aussage zur Kryptographie im Interesse der Sicherheitsbehörden vermeiden wollten oder eine Richtlinienkompetenz des Rates und des Parlaments in diesem Bereich abgelehnt haben. Positiv ist zu bewerten, daß der Gemeinsame Standpunkt den *Grundsatz der Vertraulichkeit* der Kommunikation an den Anfang der materiell-rechtlichen Regelungen stellt und ihm einen hohen Stellenwert zuweist. Zu begrüßen ist auch die *strikte Zweckbindung* von Abrechnungsdaten, die der Betreiber selbst zur Vermarktung seiner eigenen Telekommunikationsdienste nur verwenden darf, wenn der Teilnehmer eingewilligt hat.

Beim *Einzelgebührennachweis* wird den Mitgliedstaaten jetzt ein größerer Spielraum bei der Abwägung zwischen den Interessen des Anrufers und denen des Angerufenen eingeräumt. Die Verkürzung der Rufnummer des Angerufenen, die im Vorentwurf zwingend vorgeschrieben war, wird jetzt nicht mehr erwähnt. Dadurch werden Lösungen wie etwa das holländische Modell ermöglicht, bei dem jeder Teilnehmer gefragt wird, ob er mit der Aufnahme seiner Rufnummer in etwaige Einzelgebührennachweise von Anrufern einverstanden ist oder nicht.

Beim Problem elektronischer Teilnehmerverzeichnisse bleibt der Entwurf der ISDN-Richtlinie erheblich hinter dem deutschen Telekommunikationsdatenschutzrecht zurück. Vor allem fehlt im Richtlinienentwurf ein differenziertes Widerspruchsrecht, das es dem Teilnehmer ermöglicht, die Eintragung seiner Daten auf gedruckte öffentliche Kundenverzeichnisse (Telefonbücher) zu beschränken und in elektronischen Verzeichnissen (CD-ROMs) auszuschließen.

Schließlich schränkt der Gemeinsame Standpunkt zur ISDN-Richtlinie die Verwendung von Voice-Mail-Systemen und Telefaxgeräten für die Zwecke des *Direktmarketings* insoweit ein, als diese nur bei vorheriger Einwilligung der Adressaten gestattet ist. Dies geht über den zwischen dem Rat und dem Europäischen Parlament noch umstrittenen Entwurf einer Richtlinie über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz[135]. Demgegenüber soll das *Telefonmarketing* nicht in jedem Fall von der vorherigen Einwilligung des Angerufenen abhängig gemacht werden. Allerdings müssen die Mitgliedstaaten Anrufe bei Teilnehmern, die keine derartigen Anrufe erhalten möchten, unterbinden.

Die Frage, wie der *Datenschutz und die Privatsphäre im Internet* effektiv gesichert werden können, tritt immer mehr in den Vordergrund. Hierzu hat die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation nach Erörterungen in Budapest und Berlin einen Bericht mit 10 Empfehlungen (Budapest-Berlin-Memorandum)[136] erarbeitet, in dem praktische Lösungsvorschläge gemacht werden. Darin wird unter anderem auf die Problematik der Nutzung des Internet zur Übermittlung medizinischer und anderer besonders sensibler personenbezogener Daten wie auch zur Veröffentlichung polizeilicher Steckbriefe und Fahndungsaufrufe hingewiesen.

4.7.2 Einzelne Dienste

Datenschutz beim Bildschirmtext (T-Online)

Ein Petent hat sich an uns gewandt und sich darüber beschwert, daß verschiedene T-Online-Anbieter, darunter auch

[135] Gemeinsamer Standpunkt (EG) Nr. 19/95 vom 29. Juni 1995 ABlEG C 288/1

[136] Anlage 5.1

die von uns kontrollierte Deutsche Bahn AG, in ihren Angeboten personenbezogene Daten (T-Online-Nummer) erheben, obwohl dies für die Leistung – im Falle der Deutschen Bahn AG die Fahrplanauskunft – nicht erforderlich sei.

Die Stellungnahme der Deutschen Bahn AG ergab, daß die Erhebung der T-Online-Nummer im Zusammenhang mit dem dort angebotenen *„Serviceprofil“* erforderlich ist. Ein solches Profil kann von jedem Benutzer der Fahrplanauskunft freiwillig angelegt werden. Dort kann der Benutzer Festlegungen z.B. über ständig wiederkehrende Buchungsmodalitäten festlegen. Darüber hinaus sei die Erhebung der T-Online-Nummer für die Abrechnung von über das System gebuchten Leistungen (Reservierungen, Fahrkarten) erforderlich. Die Deutsche Bahn AG hat jedoch mittlerweile für den Bereich der Fahrplanauskunft auch einen anonymen Zugang ohne Buchungs- und Reservierungsmöglichkeit eingerichtet, bei dem die T-Online-Nummer des Kunden nicht erhoben wird.

Dies steht im Einklang mit den auf Bundes- und Länderebene geplanten Regelungen für Tele- und Mediendienste, in denen die Anbieter solcher Dienste verpflichtet werden, mindestens alternativ auch einen anonymen Zugang zu ihren Angeboten vorzusehen, soweit dies technisch und der Art des Dienstes nach möglich ist.

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Die Markteinführung des digitalen Fernsehens hat begonnen. Zusätzlich zu einem deutlich ausgeweiteten Programmvolumen eröffnen sich damit für die Anbieter derartiger Dienste neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen, sind mit besonderen Gefährdungen für das informationelle Selbstbestimmungsrecht der Benutzer verbunden. Je nach Ausgestaltung der Systeme besteht hier die Gefahr, daß Mediennutzungsprofile einzelner Nutzer erstellt werden, die Auskunft über individuelle Vorlieben, Interessen und Sehgewohnheiten geben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung zum Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen die Anbieter und Programmlieferanten aufgefordert, den Nutzern mindestens alternativ auch solche technischen Lösungen anzubieten, bei denen keine personenbezogenen Daten über einzelne empfangene Sendungen registriert werden können[137]. Die technischen Voraussetzungen für solche anonymen Zugangslösungen sind grundsätzlich gegeben.

Pilotprojekt „Interaktive Videodienste“ in Berlin

Das am 15. Februar 1995 in Berlin gestartete Multimedia-Pilotprojekt „Interaktive Videodienste Berlin“ der Deutschen Telekom AG, dessen Laufzeit ursprünglich auf ein Jahr befristet werden sollte, ist verlängert worden und wird nach wie vor angeboten. Immer noch ist das Berliner Pilotprojekt das einzige der ursprünglich insgesamt sechs in Deutschland geplanten Pilotprojekte, das tatsächlich den Betrieb aufgenommen hat. Die Funktionen des eingesetzten Systems und die dort angebotenen Dienste hatten wir bereits im letzten Jahresbericht beschrieben[138].

Geprüft wurde, welche personenbezogenen Daten über die *Inanspruchnahme einzelner Dienste* im Berliner Pilotprojekt, an

[137] vgl. Anlage 2.7
[138] JB 1995, 4.2

dem neben öffentlichen Einrichtungen auch Privatpersonen teilnehmen, erhoben und verarbeitet werden. Daten über die Nutzung der – nach wie vor ausnahmslos kostenfrei angebotenen – Dienste durch die Teilnehmer werden in der Betriebszentrale des Pilotprojekts verschlüsselt erfaßt. Der Schlüssel für die Zuordnung der Nutzungsdaten zu den einzelnen Teilnehmern ist nur einem begrenzten Personenkreis bekannt. Eine Auswertung des Nutzerverhaltens erfolgt nur für die mit dem Pilotprojekt verfolgten Zwecke. Eine Weitergabe von Nutzerdaten an Dritte ist grundsätzlich ausgeschlossen.

Die Verarbeitung und Nutzung personenbezogener Daten der Teilnehmer ist nur auf Grundlage und im Rahmen von deren Einwilligung möglich, die einschlägigen Vorschriften der §§ 47, 58 des Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks[139] erlauben eine Verarbeitung personenbezogener Daten über die Nutzung einzelner Angebote nicht. Die Einwilligung ist bei den am Pilotprojekt teilnehmenden Privatpersonen von der Telekom eingeholt worden.

Die ursprünglich im Rahmen der Pilotprojekte geplante Erprobung von anonymen Nutzungsformen hat bislang nicht stattgefunden. Insgesamt muß die Zukunft der Pilotprojekte „Interaktive Videodienste“ als ungewiß bezeichnet werden. Dies gilt insbesondere, nachdem das technisch ambitionierte *Stuttgarter Pilotprojekt*, für das die Beteiligung einer wesentlich größeren Anzahl von Nutzern als im Berliner Pilotprojekt geplant war, gescheitert ist. Darüber hinaus hat es den Anschein, als seien einige der angebotenen Dienste – insbesondere der *Video-on-demand-Dienst*, bei dem einzelne Angebote von einem Video-Server abgerufen werden können – technisch noch nicht bis zur Marktreife gelangt. Auch die gleichzeitige Einführung des digitalen Fernsehens dürfte die Marktchancen von interaktiven Videodiensten für die nahe Zukunft schmälern.

4.8 Informationstechnische Verfahren und Informationssicherheit

4.8.1 Informationstechnische Infrastruktur

Die moderne Kommunikationsinfrastruktur der Berliner Verwaltung ist zunächst im Rahmen zweier getrennter Projekte, den Projekten zum Aufbau des Metropolitan Area Networks (MAN) für die Datenkommunikation und des ISDN-Vernetzungskonzeptes für die Fernsprechkommunikation, entwickelt worden.

Zu Beginn des Jahres wurden die beiden Einzelprojekte in einem neuen gemeinsamen Projekt *„Berliner Landesnetz (BeLa)“* zusammengefaßt. Entgegen der ursprünglichen Planung soll das BeLa als integriertes Daten- und Fernsprechnetz realisiert werden und damit eine gemeinsame Nutzung der Lichtwellenleitungen des MAN und des ISDN-Netzes erfolgen. Die damit verbundene Aufhebung der bisherigen physikalischen Trennung der Netze bringt sicherheitstechnische Auswirkungen auf die bisherige Konzeption mit sich. Für die bisher geplanten Netze wurden jeweils eine Risikoanalyse und ein darauf aufbauendes Datenschutz- und Datensicherheitskonzept zur Minimierung der Risiken erarbeitet, zu denen wir uns in früheren Jahresberichten auch schon geäußert haben[140].

Nun muß geprüft werden, inwieweit die Datenschutz- und Datensicherheitskonzepte an die neuen Rahmenbedingungen

Die Abschottung der Netze für die Sprachkommunikation und für die Datenkommunikation wird zumindest aus Richtung

[139] GVBl. 1992, S. 151 ff.
[140] JB 1994, 2.2, JB 1995, 2.2

angepaßt werden müssen und insbesondere, ob durch die Integration neue, bisher nicht beachtete Risiken entstehen. Hierbei muß vor allem die Abschottung der Datenkommunikation von der Fernsprechkommunikation beachtet werden. Dabei ist zu berücksichtigen, daß durch die Integration zwar Kommunikationswege zwischen verschiedenen Stellen für die Fernsprechkommunikation geöffnet werden müssen, zwischen denen aber eine Datenkommunikation unzulässig ist und daher mit technischen Mitteln zu unterbinden ist.

Aufgrund der derzeitigen Haushaltslage des Landes Berlins wurde der Schwerpunkt auf das Teilprojekt „ISDN“ gelegt, dessen oberste Priorität die Kostensenkung der Fernsprechdienste der Berliner Verwaltung darstellt.

Noch immer Löcher im Berliner Verwaltungsnetz

Die zunehmende Nutzung des *Berliner Verwaltungsnetzes (MAN)* durch die einzelnen Verwaltungen und Verfahren zeigt verstärkt Sicherheitsprobleme innerhalb des Verwaltungsnetzes auf. Die anfängliche Euphorie, eine einfache, kostengünstige und schnelle Kommunikation zwischen den Verwaltungen und innerhalb der Verfahren zu erhalten, weicht zunehmend der Erkenntnis, daß die Sicherheit des Netzes erheblich mehr Aufwand und Kosten verursacht, als zunächst von den meisten angenommen wurde.

Das Datenschutz- und Datensicherheitskonzept für das MAN schlägt eine große Anzahl von Maßnahmen vor, die insgesamt ein ausreichendes Sicherheitskonzept ergeben. Jedoch wurde der Umsetzung dieser Sicherheitsanforderungen keineswegs die Priorität eingeräumt, die ihr angemessen ist. Demgegenüber scheint der Umsetzung von sicherheitsbedürftigen bzw. risikoerzeugenden Verwaltungsverfahren auf dem MAN mehr Bedeutung zugemessen zu werden. So wird zum Beispiel beabsichtigt, mit der *Senatsbibliothek* einen ersten *Pilotversuch* zur Nutzung des Internet über das MAN durchzuführen. Auch wenn es sich dabei nur um Anfragen zu verfügbaren Werken – und damit noch nicht um die datenschutzrechtlich hochrelevante Ausleihe – handeln sollte, wird das MAN dadurch zum Internet geöffnet. Voraussetzung dafür sollte es jedoch sein, daß einerseits vorher das Datenschutz- und Datensicherheitskonzept vollständig umgesetzt ist und andererseits ein gestaffeltes Firewall-System realisiert wurde, das den hohen Sicherheitsanforderungen entspricht. Allerdings kann auch ein solches optimales Firewall-System keine hundertprozentige Sicherheit gegen Angriffe aus dem Internet erzeugen, da ständig neue und unerwartete Angriffsformen aus dem Internet bekannt werden, die bei Firewall-Systemen erst im Nachherein Berücksichtigung finden können.

Die Erfahrungen dieses Jahres haben jedoch gezeigt, daß die Mindestvoraussetzungen für die Sicherheit im MAN nicht gegeben sind.

So traten innerhalb eines Großverfahrens erhebliche Sicherheitsprobleme auf, weil nicht ausgeschlossen werden konnte, daß man über das *Network File System (NFS)* von beliebigen UNIX-Servern im MAN aus unbefugt auf die Verfahrens-Server zugreifen konnte. Dabei ist aus der Fachliteratur bekannt, daß NFS aufgrund seiner bekannten Sicherheitsproblematik nur innerhalb von lokalen Netzen und nicht über deren Grenzen hinweg eingesetzt werden sollte. Hinzu kam, daß Konfigurationsmöglichkeiten für die Nutzung von NFS, die die Risiken zumindest hätten vermindern können, innerhalb des MAN nicht realisiert worden waren. Als die Sicherheitslücke bekannt wurde, wurde umgehend eine Arbeitsgruppe im LIT eingesetzt, die konkrete Maßnahmen zur Lösung des Problems

Sprache durch technische Mittel allein nicht gelingen. Die Integration von ISDN und Intelligent Network (IN) Komponenten im Endgerätebereich beruht ja gerade auf solchen Übergängen. Den Belangen der Netzsicherheit kann hier nur dann genügend Rechnung getragen werden, wenn die möglichen Schnittstellen zwischen diesen Netzen und die daraus abgeleiteten Bedrohungen bei der Erstellung des Sicherheitskonzepts für das Gesamtnetz berücksichtigt werden.

Das Datenschutz- und Datensicherheitskonzept für das Berliner MAN schlägt eine große Anzahl von technischen und organisatorischen Maßnahmen vor, die insgesamt ein sicheren Netzbetrieb ermöglichen. Die Umsetzung der jeweiligen Sicherheitsanforderungen ist weitestgehend abgeschlossen. Dies betrifft insbesondere die Sicherheitsanforderungen an die logische Netzebene, Vereinbarungen, Teststrategien, Ausbildungspläne und Fernadministration. Zur Zeit werden alle Anstrengungen unternommen, um die Sicherheitsanforderungen für die physikalische Netzinfrastruktur umzusetzen. Trotz hoher Priorität konnten in diesem Bereich bisher nicht alle Maßnahmen umgesetzt werden, da die erforderlichen Mittel auf Grund der angespannten Haushaltssituation nicht immer rechtzeitig zur Verfügung standen.

Der im Bericht erwähnte Pilotversuch wurde in dieser Form nicht realisiert. Der Zugang zum Internet und zu Fremdnetzen aus dem Verwaltungsnetz heraus wird in 2 Stufen erfolgen:

1. Separates Grenznetz, d.h. Zugang nur über TK und X.25 und
2. Gesicherte Anbindung des Grenznetzes an das Verwaltungsnetz.

Mit dem stufenweisen Vorgehen werden sowohl für das Landesamt für Informationstechnik als Betreiber, als auch für die IT-Anwender die Risiken und ihre Beherrschung handhabbar.

Die angesprochenen Arbeitsgruppe hat folgende Lösungen erarbeitet und den betroffenen Institutionen zugänglich gemacht:

- Sperrung der durch NFS benutzten Ports im MAN, soweit dies unter Beachtung der Kommunikationsbeziehungen möglich ist. Dadurch ist im allgemeinen der Einsatz von NFS nur noch in den lokalen Netzen möglich.
- Erarbeitung von Konfigurationshinweisen für die im Land Berlin eingesetzten UNIX-Systeme, in denen die Möglichkeiten, die NFS zur Erlangung von Sicherheit bietet, eingesetzt werden (Export nur an bestimmte Adressen).
- Erarbeitung von Shellscripten, die eine zeitliche Begrenzung des Zuganges zu NFS ermöglichen (keine exportierten File-

ausarbeiten und umsetzen sollte.

Aus diesem Beispiel wird die eigentliche Problematik ersichtlich: Das MAN wird als *transparentes Transportmedium* angesehen, d.h. es überträgt, was ihm zur Übertragung übergeben wird, und setzt nur wenige formale Rahmenbedingungen voraus. Die datenschutzrechtliche Verantwortung für die Übertragung personenbezogener Daten im MAN liegt bei den Anwendern. Dieses bedeutet, daß der Netzbetreiber LIT zwar Sicherheitsmechanismen anbieten kann, ihre Nutzung und eventuelle Ergänzung aber um zusätzliche Sicherheitsmaßnahmen von den Verantwortlichen der angeschlossenen Teilnetze und den Verfahrensbetreibern erfolgen müssen. Die Verfahrensbetreiber und damit die Nutzer des MAN werden sich dieser Verantwortung hierfür jedoch erst jetzt langsam bewußt.

Ein weiteres Beispiel ist das Automatisierte Haushaltswesen (AHW). Den Verfahrensbetreibern wurde klar, wie einfach es ist, mit „Netzabhörprogrammen“ („*Packet Sniffer*“[141]), die für wenig Geld direkt aus dem Katalog bestellt werden können, unverschlüsselte Paßwörter herauszufiltern. Beim automatisierten Haushaltswesen stehen zwar keine personenbezogenen Daten im Vordergrund, jedoch birgt der eventuell mögliche unbefugte Zugang zum eigentlichen Haushaltsverfahren des Landes ein erhebliches Risiko in sich, da mit dem unbefugten Zugriff auch Risiken für die Verfahrensintegrität gegeben sind. Die Risiken werden völlig unkontrollierbar bei einer Internet-Anbindung des MAN, da dann solche Angriffe von jedem Ort der Welt möglich sind.

Ein großes Problem ist in der *unverschlüsselten Übertragung* personenbezogener Daten über das MAN zu sehen. Um die Vertraulichkeit und Integrität personenbezogener Daten zu gewährleisten, dürfen diese nur verschlüsselt über das MAN übertragen werden. Die Verantwortung hierfür tragen die Verfahrensbetreiber und damit die Nutzer des MAN. Dieses stellt insbesondere die „Altverfahren“ vor Probleme, da es oftmals nur bedingt möglich ist, bestehende Programme um Verschlüsselungsmechanismen zu erweitern.

Eine Lösung bieten *„black boxes“* an, die eine Verschlüsselung auf Netzebene ermöglichen. Trotz des finanziellen Aufwandes müssen derartige Verfahren eingesetzt werden. Für die aktuell in der Konzeptionierung und Realisierung befindlichen und allen zukünftigen Verfahren sollte eine einheitliche Sicherheitsstrategie, wie sie z.B. durch Nutzung der entsprechenden DCE-Mechanismen möglich wäre, erarbeitet und umgesetzt werden.

Sehr positiv ist zu vermerken, daß ein *Arbeitskreis Netzsicherheit* im LIT initiiert wurde, der die Probleme erörtert

systeme außerhalb der Geschäftszeiten).

Durch Einsatz dieser Maßnahmen ist eine deutliche Reduzierung der Risiken des Einsatzes von NFS möglich.

Im Verlauf der Erarbeitung von Lösungen zur Risikoverminderung des NFS-Einsatzes wurde das im Intranet der Berliner Verwaltung zur Verfügung stehende Newssystem um zwei Newsgruppen erweitert, die speziell für Information und Diskussion zum Thema Sicherheit benutzt werden (lit.security.cert enthält die Sicherheitshinweise des CERT, lit.security dient als allgemeines Diskussionsforum für Sicherheitsbelange).

Die Darstellung des Berliner Datenschutzbeauftragten ist in der Sache richtig. Ergänzend muß darauf hingewiesen werden, daß es sich hierbei nicht um ein spezielles Problem des AHW sondern um ein grundsätzliches Problem des Netzbetriebes, das für alle Anwendungen im Land Berlin gilt, handelt. Vor diesem Hintergrund wird gegenwärtig von der Senatsverwaltung für Finanzen in Abstimmung mit anderen Nutzern des MAN (u.a. SenInn, LIT, SenBauWohnV, BA Schöneberg) sowie dem Berliner Datenschutzbeauftragten und dem Rechnungshof von Berlin nach einer OSI-konformen Lösung (DCE-Security) gesucht, die das Sicherheitskonzept für das AHW mit der Standardsoftware PROfiskal® angemessen ergänzt und zugleich auf andere Großverfahren übertragbar ist. In die Erarbeitung einer Lösung sind externe Sicherheitsexperten einbezogen, die bereits die Risikoanalysen für das AHW durchgeführt und das Sicherheitskonzept maßgeblich entwickelt haben. Ungeachtet dessen hält es der Senat aber im Hinblick auf eine sinnvolle Risikominderung für wenig hilfreich, im Vorfeld einer sich abzeichnenden Lösung derartige Sicherheitslücken zu publizieren und damit Neugierde in einer breiten Öffentlichkeit zu erwecken.

Die endgültige Auswahl einer Lösung ist bisher durch den Verfahrensbetreiber nicht erfolgt. Da mehrere hundert Arbeitsplätze im Land Berlin betroffen sind, bedarf es einer genauen Analyse aller möglichen Varianten, um so die optimale Lösung (Sicherheit, Kosten und Administrationsaufwand) zu ermitteln.

Das technische Vorhaben Grenznetz ist in das Sicherheitskonzept Backbone-Dienste des Landesamtes für Informationstechnik eingebunden. Danach haben das Landesamt für Informationstechnik und IT-Anwender gemeinsam im Sicherheitskonzept für die am Backbone angeschlossenen Verfahren geeignete Maßnahmen zu treffen, um die Sicherheit zu gewährleisten. An dieser Stelle hört das Backbone für Verfahren mit einem höheren als dem mittleren Schutzbedarf auf, reines Transportmedium zu sein. Diese Verfahren müssen dem Landesamt für Informationstechnik mit ihren

[141] JB 1995 4.1

und die Lösungsmöglichkeiten koordiniert. In diesem Arbeitskreis arbeitet auch der Berliner Datenschutzbeauftragte mit.

Des weiteren wurde zur Vorbereitung der Internet-Anbindung eine Testumgebung geschaffen, die im wesentlichen das MAN widerspiegelt. In dieser separaten Nachbildung des MAN wurden verschiedene Firewalls unterschiedlicher Hersteller integriert und getestet. Durch Nutzung solcher Testumgebungen können die notwendigen Sicherheitsmaßnahmen realisiert und auch mit Hilfe externen „Hacker"-Sachverstands – ausgetestet werden.

sicherheitsrelevanten Anforderungen bekanntgemacht werden, um dafür entsprechend vereinbarte Sicherheitsdienste zu erbringen. Das Landesamt für Informationstechnik hat dazu in dem o.g. Sicherheitskonzept einen Produktkatalog angegeben.

Der Einsatz von Kryptoboxen wird vom Landesamt für Informationstechnik wegen der zu hohen Aufwendungen nicht empfohlen. Das Landesamt orientiert sich in der Projektierungsphase auf den Einsatz von DCE bzw. auf den Einsatz von Sicherungsfunktionen, die über den BermanAccessService – ein vom Landesamt für Informationstechnik zur Verfügung gestellter Sicherheitsservice – und für vorgegebene Verfahren auf die Anwendung der VPN-Technologie. Die VPN-Technologie wird als Zusatzoption der ohnehin einzusetzenden Firewall-Technik verfügbar. Das Problem der Herstellerabhängigkeit wird damit aber ebenso wie bei den Kryptoboxen nicht gelöst.

4.8.2 Informationssicherheit in der Berliner Verwaltung

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den letzten Jahren veröffentlichten Verfahren zur Erarbeitung von *IT-Sicherheitskonzepten*, das *IT-Sicherheitshandbuch* und das jährlich ergänzte und überarbeitete *IT-Grundschutzhandbuch* bilden auch in Berlin eine wichtige Grundlage zur Erarbeitung von Risikoanalysen und darauf aufbauenden Sicherheitskonzepten. Soweit solche Konzepte für Systeme und Verfahren in der Berliner Verwaltung entwickelt worden sind, waren sie weitgehend zufriedenstellend. Was indes meist fehlte, war die konsequente und rechtzeitige Umsetzung solcher Konzepte.

Die Senatsverwaltung für Inneres hat die Anwendung des Handbuchs in den Behörden nachdrücklich empfohlen und angekündigt, daß die sich aus den speziellen Anforderungen der Berliner Verwaltung ergebenden Konkretisierungen und Anpassungen schnellstmöglich erarbeitet werden[142].

Das IT-Grundschutzhandbuch ist mittlerweile ein von vielen Behörden der Berliner Verwaltung genutztes Arbeitsmittel zur Erstellung und Umsetzung von IT-Sicherheitskonzepten. Die aktuelle Fassung wurde als CD-ROM an alle Bezirks- und Senatsverwaltungen verteilt und ist außerdem über das Intranet als WWW-Dokument verfügbar.

In dem Rundschreiben wird auch der wichtige Hinweis gegeben, daß die Maßnahmenempfehlungen des IT-Grundschutzhandbuches nur für den *mittleren Schutzbedarf* gelten können. Wann dieser mittlere Schutzbedarf ausreichend ist und wann nicht mehr, ist im Einzelfall festzustellen. Dazu bietet das IT-Grundschutzhandbuch Handreichungen. Soweit nicht mehr vom Grundschutz ausgegangen werden kann, wäre das IT-Sicherheitshandbuch anzuwenden, mit dem differenziertere Risikobetrachtungen möglich sind und somit genauere, das heißt weniger pauschale Konzepte entwickelt werden können. Allerdings ist der Auswand für ein Verfahren nach dem IT-Sicherheitshandbuch ungleich höher.

Die Anwendung des IT-Grundschutzhandbuchs und die Umsetzung der damit erarbeiteten Sicherheitskonzepte führt im Vergleich zur bisherigen Situation zu einem befriedigenden Sicherheitsniveau. Daher ist es zu begrüßen, wenn das IT-Grundschutzhandbuch bei personenbezogenen Verfahren, die normalen IT-Sicherheitsrisiken unterliegen, regelmäßig eingesetzt wird.

Bei Großverfahren, deren Daten besonderen Amtsgeheimnissen oder anderen besonderen Sicherheitsanforderungen unterliegen oder bei denen aufgrund der eingesetzten Technik besondere Risiken anzunehmen sind, kann dagegen zwar für wesentliche Teile des Sicherheitskonzeptes ebenfalls vom Grundschutz ausgegangen werden, für andere aber nicht, so daß eine zumindest partielle Anwendung des IT-Sicherheitshandbuches ange-

[142] Rundschreiben vom 9. Januar 1996 zur Anwendung des IT-Grundschutzhandbuches

messen ist.

Dies kann man an folgenden bereits erwähnten Verfahren zeigen:

Das *Berliner Landesnetz* dient dem Transport von Daten fast aller Berliner Verfahren, so daß davon ausgegangen werden muß, daß auch Daten übertragen werden, die hinsichtlich der Verfügbarkeit, Integrität und/oder Vertraulichkeit höchsten Schutzbedarf aufweisen. Daher war es auch angebracht, das IT-Sicherheitskonzept vollständig auf der Grundlage des IT-Sicherheitshandbuchs durchzuführen. Das gleiche gilt für andere Infrastrukturen, die für die Verarbeitung nicht vorher bestimmbarer Daten benutzt werden.

Das im Aufbau begriffene *Integrierte Personal-Verfahren (IPV)* und das *Berliner Automatisierte Sozialhilfe-Interaktions-System (BASIS)* arbeiten mit personenbezogenen Daten, die dem Personaldaten- bzw. Sozialgeheimnis unterliegen. Zumindest hinsichtlich der Vertraulichkeit und Integrität der Daten kann daher nicht mehr vom Grundschutz ausgegangen werden.

Das modernisierte Verfahren des *Automatisierten Haushaltswesens (AHW)* verarbeitet kaum Daten, deren Vertraulichkeit überdurchschnittlichen Schutzbedarf aufweist. Sie betreffen finanzielle Transaktionen, so daß besonders hohe Anforderungen an ihre Integrität zu stellen sind.

Für das AHW liegt ein mit externer Unterstützung erstelltes Sicherheits- und Betriebskonzept vor, das die Billigung des Berliner Datenschutzbeauftragten gefunden hat und bei Bedarf fortgeschrieben wird. In Zusammenhang mit der vom Berliner Datenschutzbeauftragten richtigerweise in den Vordergrund gestellten Datenintegrität verweist der Senat auf seine oben unter Nr. 4.8.1 („Noch immer Löcher im Berliner Verwaltungsnetz“) gemachten Ausführungen zu PROfiskal® im Netzbetrieb.

Beim *Polizeilichen Einsatzleitsystem (PELZ)* kommt es in erster Linie auf die Verfügbarkeit des Systems, der Programme und Daten an, so daß zumindest in dieser Hinsicht eine Orientierung am Grundschutz verfehlt wäre.

Die Beispiele zeigen, daß *differenzierte Risikobetrachtungen* eine zwingende Voraussetzung dafür sind, daß Sicherheitskonzepte entwickelt und umgesetzt werden, die an den jeweiligen Bedarf angepaßt sind. Dies bedeutet, daß keine teuren Maßnahmen dort ergriffen werden, wo sie keine entsprechende Auswirkung auf die IT-Sicherheit haben, aber dort gezielt investiert werden kann, wo dies zur Abwehr von Bedrohungen auch erforderlich ist. Die Risiken hängen nicht nur von der Art der Daten und Verfahren, sondern auch von den jeweiligen technischen, organisatorischen und räumlichen Verhältnissen ab, so daß stets Einzelfallbetrachtungen erforderlich sind. Pauschale Datenschutz- und IT-Sicherheitskonzepte, die sich an ebenso pauschalen Schutzstufen orientieren, halten wir daher für verfehlt.

Mittlerweile ist von der Senatsverwaltung für Inneres im Rahmen der IT-Strategie des Landes der Entwurf für ein *Rahmenkonzept zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (Sicherheitsrahmenkonzept)* vorgelegt worden. Dieses Rahmenkonzept

Das vom Berliner Datenschutzbeauftragten ausdrücklich begrüßte Konzept ist die Grundlage für alle weiteren notwendigen Aktivitäten zur Gewährleistung von IT-Sicherheit beim IT-Einsatz in der Berliner Verwaltung und hat bereits in den Behörden ein breites Echo gefunden.

- definiert die Grundsätze der Sicherheitspolitik im Sinne der vom BSI herausgegebenen Handbücher,
- beschreibt die Rollen eines dezentralen und eines zentralen IT-Sicherheitsmanagements und die Sicherheits-Verantwortlichkeiten der am IT-Einsatz beteiligten Anwender, Verfahrensverantwortlichen und Infrastrukturbetreiber,
- definiert Sicherheitsdomänen als funktional, organisatorisch und räumlich zusammengehörige Bereiche, für die einheitliche Sicherheitsanforderungen bestehen und für die ein einheitliches IT-Sicherheitskonzept zu erstellen und

[143] siehe Abschnitt 2.2
[144] vgl. 2.3
[145] Dies entspricht den Anforderungen der „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

umzusetzen ist,
- verlangt als Mindeststandard für behördenbezogene Sicherheitskonzepte den Grundschutz auf der Grundlage der Anwendung des IT-Grundschutzhandbuches,
- fordert für IT-Verfahren, für die mehr als mittlerer Schutzbedarf zu fordern ist, die Erstellung des IT-Sicherheitskonzeptes auf der Grundlage des IT-Sicherheitshandbuchs, ggf. unter Einbindung externen Sachverstands,
- verlangt im Sinne der Ideen zu den „Privacy enhancing Technologies“[143] die Separierung von Pseudonymitäts- und Identitätssphären sowie die Anonymisierung und Pseudonymisierung personenbezogener Daten, soweit machbar,
- verlangt bei der Übertragung von schutzwürdigen Daten die Verschlüsselung mindestens in der Stärke des DES[144],
- verlangt insbesondere bei der Übertragung von Paßwörtern und sonstigen Authentifizierungsdaten eine Verschlüsselung,
- verlangt bei der Nutzung des Internet die strenge Orientierung an einem restriktiv orientierten Kommunikationsbedarf, die Umsetzung eines schlüssigen Sicherheitskonzepts, die Nutzung einer zentral bereitgestellten Firewall sowie gestaffelte Firewalls zur Absicherung spezieller Sicherheitsdomänen[145],
- fordert die Einrichtung geschlossener Benutzergruppen zur Verhinderung unbefugten Zugriffs auf IT-Verfahren,
- verlangt das Angebot applikationsneutraler Sicherheitsdienste als Bestandteil dezentraler oder zentraler Infrastrukturdienste,
- beschränkt die Benutzung von Programmen auf freigegebene Programme,
- erwartet, daß die Systeme sich gegenüber ungewollter Fehlbedienung fehlertolerant verhalten,
- verlangt geeignete Schulungsmaßnahmen zur Schaffung eines grundlegenden Sicherheitsbewußtseins bei den am IT-Einsatz beteiligten Mitarbeitern und die Berücksichtigung IT-sicherheitsrelevanter Inhalte bei allen spezifischen IT-Schulungsmaßnahmen.

Dieses Rahmenkonzept haben wir nachdrücklich begrüßt, weil es alle wesentlichen derzeit bekannten Erkenntnisse zur Gewährleistung von IT-Sicherheit in modernen IT-Infrastrukturen berücksichtigt.

4.8.3 PC- und Netzanwendungen

In diesem Berichtsjahr wurden verstärkt datenschutzrechtliche Kontrollen von PC- und Netzanwendungen (z.B. Novell, WindowsNT, Workgroup-Netze, Novell-lite) durchgeführt. Dabei stand die Wirksamkeit von technischen und organisatorischen Maßnahmen zur Minimierung von Risiken hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit bei der Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung und der privaten Wirtschaft im Vordergrund.

Die Auswertung der Ergebnisse ergab gravierende Unterschiede bei der Umsetzung der vom Gesetzgeber geforderten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. So konnten wir uns bei einigen Anwendern darauf beschränken, ergänzenden Empfehlungen hinsichtlich der Verfahrensabwicklung zu geben, während bei anderen wegen grober Mängel Beanstandungen ausgesprochen werden mußten.

Die Analysen der durchgeführten Kontrollen vermitteln ein differenziertes Bild, wenn man danach unterscheidet, ob die Verfahren auf Einzelplatz-PCs oder innerhalb einer Netzkonfiguration ablaufen. Während die Maßnahmen zum Datenschutz beim Einsatz von Einzelplatz-PCs häufig als unzureichend eingeschätzt werden mußten, fiel die Bewertung bei den Netzen deutlich besser aus.

Bei der Entwicklung von Betriebssystemen für Einzelplatz-

Zahlreiche in dem Abschnitt enthaltene Empfehlungen werden durch entsprechende Anforderungen und Maßnahmen aus dem für die Anwendung in der Berliner Verwaltung empfohlenen IT-Grundschutzhandbuch bereits abgedeckt. Die weitergehenden Empfehlungen werden von der zuständigen Senatsverwaltung auf ihre technisch-organisatorische Machbarkeit geprüft und können, soweit sie nicht ausschließlich lokale Aspekte des IT-Einsatzes betreffen, in geeigneter Weise bei der Fortschreibung unseres Rahmenkonzeptes berücksichtigt werden.

PCs wurden die Aspekte von Datenschutz und Datensicherheit nicht oder kaum berücksichtigt. Gerade das immer noch sehr verbreitete Betriebssystem MS-DOS und seine grafische Benutzeroberfläche MS-Windows weist viele Sicherheitslücken auf. Zudem wurden selbst die Optionen, die einen gewissen Schutz bieten könnten, nicht genutzt. Dies geschah zumeist aus Unkenntnis, da diese Schutzeigenschaften von den Herstellerfirmen in den Handbüchern nicht oder nur unzureichend beschrieben werden und meist entsprechenden Fachzeitschriften entnommen werden müssen. Ohne zusätzliche Sicherheitsprodukte läßt sich das System jederzeit in Betrieb nehmen und gestattet dem Nutzer unter Umständen den uneingeschränkten Zugriff auf alle gespeicherten Daten. Doch auch der Einsatz von Sicherheitstools gewährleistet keinen hinreichenden Schutz der personenbezogenen Daten, wenn deren Installation nur lückenhaft konzipiert und umgesetzt wird.

In dieser Hinsicht sind Netzbetriebssysteme wie Windows NT und Novell Netware von vornherein besser ausgestattet. Jedoch hat sich auch hier gezeigt, daß durch eine nicht ordnungsgemäß bzw. unvollständig durchgeführte Installation die in das System implementierten Schutzmechanismen nicht wirksam werden können.

Der Maßstab für unsere Kontroll- und Beratungsaktivitäten findet sich in den zehn Kontrollanforderungen, die in § 5 Abs. 3 BlnDSG bzw. ähnlich in der Anlage zu § 9 BDSG für die automatisierte Verarbeitung personenbezogener Daten festgeschrieben wurden. So soll im folgenden anhand der dort geforderten technischen und organisatorischen Maßnahmen eine Übersicht über festgestellte Mängel bzw. unsere Empfehlungen gegeben werden:

Zugangskontrolle (Ziel: Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren): Die erforderlichen Maßnahmen (Türsicherung mit Sicherheitsschlössern, Kontrolle des Publikumsverkehrs, der Raumreinigung und der Durchführung von Wartungsarbeiten) wurden im wesentlichen eingehalten. Auch die Anforderungen hinsichtlich der Unterbringung von Servern wurden zumeist vorbildlich umgesetzt (besonders geschützte Räume in Obergeschossen, bei unumgänglicher Installation im Erdgeschoß bauliche Außensicherungen). Teilweise waren sogar Bewegungs- und/oder Glasbruchmelder installiert. Bei der Gestaltung dieser Sicherungsmaßnahmen wurde oftmals auch polizeiliche Beratung in Anspruch genommen.

Datenträgerkontrolle (Ziel: Es ist zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können): Die Datenträger werden zwar in den meisten Fällen ordnungsgemäß gekennzeichnet, in Boxen zwischengelagert und nach Dienstende in einem verschlossenen Schrank aufbewahrt. Die Archivierung wird jedoch oftmals vernachlässigt, so daß ein revisionsfähiger Datenträgeraustausch (Eintragung in ein Ausgangs- bzw. Eingangsbuch, Ausstellung von Begleitscheinen) nicht gewährleistet ist. Mängel wurden auch bei der Überschreitung von gesetzlich vorgegebenen Aufbewahrungsfristen sowie bei der datenschutzgerechten Vernichtung von Datenträgern und nicht mehr benötigten Ausdrucken festgestellt. Vielfach wurden auch ungesicherte Diskettenlaufwerke vorgefunden, wobei derartige Mängel insbesondere im privaten Bereich zu verzeichnen waren. Nur in Ausnahmefällen konnte von uns eine Verschlüsselung von sensiblen Daten auf den Datenträgern registriert werden. Hier besteht erheblicher Nachholbedarf.

Speicherkontrolle (Ziel: Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern): Es ist systemtechnisch zu sichern, daß sich die Aktivitä-

ten der Benutzer auf solche Funktionen (Lesen, Schreiben, Löschen) beschränken, die ihrem Aufgabenspektrum entsprechen. Dazu dienen differenzierte Profile zur Bearbeitung von Dateien. Gegebenenfalls sind solche Rechte sogar bezüglich bestimmter Felder einer Datei festzulegen. Derartig fein abgestufte Nutzerprofile haben wir insbesondere bei Anwendungen auf Einzelplatz-PCs in den seltensten Fällen beobachten können, da auch ein Großteil der eingesetzten Standardprogramme diese wünschenswerten Schutzmechanismen noch nicht aufweist. Selbst wenn die Fachanwendungen einen entsprechenden Schutz vorsehen, wird dieser unter Umständen dadurch wieder aufgehoben, daß dem Nutzer der Zugang auf die Betriebssystemebene nicht verwehrt wird. Beim Einsatz von Notebooks sollte wegen des hohen Diebstahlrisikos der Schutz sogar dergestalt erweitert werden, daß sensible Daten verschlüsselt auf dem jeweils eingesetzten Speichermedium abgelegt werden.

Benutzerkontrolle (Ziel: Die Benutzung von Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern): Eine wirksame Kontrolle der Benutzer eines Datenverarbeitungssystems kann nur gelingen, wenn ihre Befugnisse den ihnen zugewiesenen Aufgaben entsprechend definiert und durch geeignete Identifikations- und Authentifikationsmechanismen sichergestellt werden. Von den auf dem Markt verfügbaren Prüftechniken (Paßwort, Chipkarten, Stimmenvergleich, biometrische Verfahren) haben wir bei unseren Kontrollen fast ausschließlich die weit verbreitete Methode vorgefunden, bei der mittels Nutzerkennzeichen und Paßwort befugte Benutzer ermittelt werden. Dabei wiesen die eingesetzten Prüfalgorithmen hinsichtlich ihrer Wirksamkeit bedeutende Niveau-Unterschiede auf. Während einige dieser Algorithmen umfangreiche Prüfungen des Paßwortes aufwiesen, mußten wir bei anderen immer noch deren Trivialität bemängeln. Selbst die als relativ schwach einzuschätzenden Schutzvorkehrungen durch die Benutzung vorhandener Schlüsselschalter zum Sperren der Tastatur oder von paßwortgeschützten Bildschirmschonern wurden häufig nicht genutzt.

Zugriffskontrolle (Ziel: Es ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können): Hier ist – analog zur Speicherkontrolle – darauf zu achten, daß befugten Benutzern eines Datenverarbeitungssystems der Zugriff lediglich auf solche Daten gestattet wird, die sie für die Erfüllung der ihnen übertragenen Aufgaben benötigen. Zu diesem Zweck sind die Zugriffsrechte restriktiv zu definieren, in geeigneter Form zu dokumentieren und im System abzubilden. Zudem ist gelegentlich zu überprüfen, ob die zugewiesenen Zugriffsrechte noch den tatsächlichen Aufgaben der Benutzer entsprechen. Insbesondere stellt sich dieses Problem bei Umsetzungen bzw. beim Ausscheiden von Beschäftigten. Auch hier ist wieder zu konstatieren, daß bei den Einzelplatzanwendungen diese Schutzfunktion ohne zusätzliche Sicherheitstools kaum gewährleistet ist. Demgegenüber bieten die gängigen Betriebssysteme für Netze von sich aus bereits Möglichkeiten, Zugriffsrechte hinreichend differenziert zu vergeben und zu prüfen.

Übermittlungskontrolle (Ziel: Es ist aufzuzeichnen, an welche Stellen wann welche personenbezogenen Daten übermittelt worden sind): Während an den Arbeitsplätzen im Netz eine derartige Protokollierung im allgemeinen vorbildlich durchgeführt wird, ist diese beim Einsatz eines Modems oder einer ISDN-Verbindung am Einzelplatz zumeist unzureichend realisiert, obwohl auch hier schon spezielle Lösungen (z.B. für den medizinischen Bereich) angeboten werden.

Eingabekontrolle (Ziel: Es ist zu gewährleisten, daß nachträglich überprüft werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverabeitungssysteme eingegeben worden sind): Ein häufig festgestellter Mangel offenbarte sich in dem Verzicht auf die vom Gesetzgeber geforderte Eingabekontrolle. Die damit verbundene Protokollierung dürfte bei dem heutigen Stand der Technik eigentlich selbstverständlich sein, da es mittlerweile diverse Softwareprodukte gibt, die eine automatisierte Aufzeichnung der Eingabeaktivitäten gestatten. Meist gewährleistet bei Einzelplatzsystemen nur der Einsatz einer Sicherheitssoftware die Ordnungsmäßigkeit der Eingabekontrolle, während bei den neueren Betriebssystemen für Netzwerke, wie z.B. Novell 4.xx oder Windows NT, diese Funktion schon integriert ist. Allerdings mußten wir feststellen, daß diese Funktion selbst in den Fällen deaktiviert war, in denen sie vom eingesetzten System angeboten wurde.

Auftragskontrolle (Ziel: Es ist zu gewährleisten, daß personenbezogene Daten , die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können): Da bei unseren Kontrollen keine Auftragsdatenverarbeitung vorgefunden wurde, konnten wir vor Ort auch keine Prüfungen zur Ordnungsmäßigkeit durchführen. Zur teilweise geplanten Vergabe derartiger Aufträge wurden Empfehlungen ausgesprochen, bei denen auf die sorgfältige Vertragsgestaltung und Auswahl des Vertragspartners, stichprobenweise Kontrollen der Ausführung des Vertrages und andere Anforderungen an die Auftragsdatenverarbeitung hingewiesen wurde.

Transportkontrolle (Ziel: Es ist zu gewährleisten, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können): Der Transport von Datenträgern wurde fast ausschließlich durch eigenes Personal in verschlossenen Behältnissen und mit Begleitscheinen durchgeführt. Dies ist ausreichend. Eine Transportkontrolle auf Datenfernübertragungswegen ist zwar grundsätzlich nur durch den Einsatz von Verschlüsselungsverfahren möglich. Davon kann aus Gründen der Verhältnismäßigkeit in lokalen Netzwerken aber abgesehen werden, wenn die Übertragungsstrecken nur über gesicherte Verkabelungen geführt werden, die vor Manipulation geschützt sind. Dies wurde bei den untersuchten lokalen Netzen meist auch vorgefunden.

Organisationskontrolle (Ziel: Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.): Die Organisation ist so zu gestalten, daß die datenschutzrechtlichen Anforderungen angemessen umgesetzt werden. Ziel der Maßnahmen im Rahmen der Organisationskontrolle ist die Unterstützung (z.B. der einzelnen Fachabteilungen) bei der Umsetzung der in den Nrn. 1 bis 9 genannten gesetzlichen Forderungen (z.B. Einrichtung der Zugriffsberechtigungen). Dabei geht es im wesentlichen um das Vorhandensein organisatorischer Regelungen, die die jeweiligen Befugnisse bei der Datenverarbeitung regeln, denn die übrigen neun Kontrollanforderungen setzen eine klare Unterscheidbarkeit zwischen befugter und unbefugter Nutzung voraus. Ferner geht es um alle Maßnahmen, die die Transparenz und damit die Kontrollierbarkeit der Datenverarbeitung bewirken. Hier wurde hauptsächlich bei kleineren privaten Unternehmen die fehlende bzw. unvollständige System- und Verfahrensdokumentation bemängelt. In der öffentlichen Verwaltung fanden wir im Gegensatz dazu häufig sogar zusätzliche Arbeitsanweisungen vor, die eine datenschutzgerechte Arbeit unterstützen.

Über die zehn Gebote hinaus ist zu empfehlen:

– Die vorhandenen *Sicherheitsoptionen*, die das Betriebssystem bietet, sollten ausgenutzt werden. Dies gilt insbesondere für die Betriebssysteme für Netze, bei denen die Sicherheit schon bei der Einrichtung der Festplatte mit einem speziellen Dateisystem (z.B. NTFS) beginnt.
– Beim Einsatz von *Notebooks* sollten die personenbezogenen Daten verschlüsselt werden, da hier eine Zugangskontrolle, wie sie die herkömmliche Büroumgebung (z.B. Ausstattung der Zimmertüren mit Sicherheitsschlössern) bietet, nicht immer möglich ist.
– Da viele Betriebssysteme Sicherheitslücken aufweisen, ist oft der Einsatz einer zusätzlich zu installierenden *Sicherheitssoftware* notwendig. Dies trifft auch dann zu, wenn mehrere Personen an einem Einzelplatz-PC arbeiten, da z.B. MS-DOS keine Benutzerverwaltung berücksichtigt.
– Beim Einsatz von Netzen ist als *Netztopologie* das Sternnetz zu bevorzugen, da hier die Daten für sämtliche Verbindungen über einen Knoten – der wie ein Server zu schützen ist – zur entsprechenden Zieladresse übertragen werden. Als Übertragungsmedium ist der Lichtwellenleiter am besten geeignet, da er eine sehr hohe Abhörsicherheit – ein Einkoppeln in den Lichtleiter ist im allgemeinen auszuschließen – ermöglicht und eine Beeinflussung durch elektrische oder elektromagnetische Störquellen ausscheidet.
– Wenn das *Diskettenlaufwerk* nicht für das Verfahren benötigt wird, ist es auszubauen oder zumindest so zu deaktivieren, daß kein unkontrollierter Zugriff stattfinden kann. Der ungeschützte Zugriff über das Diskettenlaufwerk stellt das größte Risiko von PC-Anwendungen dar.

4.8.4 Neue Gefahren aus dem Netz

Mit dem Aufkommen des wichtigsten Internet-Dienstes World Wide Web (WWW) sorgte eine neue *Programmiersprache Java* für Aufsehen, mit der Programme (z.B. 3D-Animationen) geschrieben werden können, die in WWW-Seiten eingebunden werden. Java ist unabhängig vom Betriebssystem, mit Java geschriebene Programme können also von beliebigen Rechnern ausgeführt werden.

Beim Aufruf einer mit einem Java-Programm versehenen Seite wird das Programm automatisch auf den abrufenden Rechner geladen und ausgeführt. Die Übertragung von ausführbaren Programmen birgt jedoch erhebliche Risiken in sich. Es ist durchaus vorstellbar, daß diese Programme „bösartig“ sein können und beispielsweise Dateien lesen, schreiben oder löschen können, ohne daß der Benutzer davon etwas bemerkt. Auch die Gefahr des Ladens von Computer-Viren oder „Trojanischen Pferden“ ist denkbar. Bekannt geworden sind auch schon Fälle, in denen die Sicherheitsmechanismen von eingesetzten Firewalls umgangen worden sind. Insbesondere die ersten Versionen der in einigen WWW-Browsern integrierten Java-Interpreter wiesen erhebliche Sicherheitsmängel auf, die im Laufe des Jahres durch neue Versionen behoben wurden. Aber auch hier entsteht die Gefahr des „Hinterher-rennens“. Ähnlich wie bei den Computer-Viren tauchen nach und nach neue Sicherheitsprobleme auf, die erst nach Bekanntwerden behoben werden können. Es ist daher unbedingt zu empfehlen, stets die neuesten Versionen der WWW-Browser zu verwenden oder aber noch besser, vorerst die Ausführung der Programme im WWW-Browser zu unterbinden.

Im Rahmen der zunehmenden kommerziellen Nutzung des Internet sind Online-Anbieter nicht mehr nur an anonymen Zugriffszahlen interessiert, sondern möchten am liebsten den gläsernen Kunden. Hierzu werden in letzter Zeit mehr und mehr

sog. *„Cookies“* verwendet. Darunter versteht man Dateien, in denen im Rechner des Nutzers auf Veranlassung des Anbieters benutzerspezifische Informationen gespeichert werden. Eine Auswertung dieser Dateien ermöglicht die Analyse des Benutzerverhaltens.

Greift ein Benutzer über seinen WWW-Browser auf einen WWW-Server zu, kann es sein, daß dieser relativ beliebige Informationen an den WWW-Browser sendet. Auf dem Computer des Benutzers werden diese Informationen in einer Cookie-Datei abgelegt. Greift der Benutzer zu einem späteren Zeitpunkt auf die gleiche WWW-Information noch mal zu, für die bereits eine Cookie-Information beim Benutzer existiert, sendet der WWW-Browser den bisherigen Cookie zum WWW-Server. Dieser kann die Cookies dann auswerten und um neue Informationen ergänzen und zurücksenden. Tauschen nun mehrere Betreiber von WWW-Servern ihre Informationen aus, können darüber umfassende Benutzerprofile erstellt werden.

Bisher blieb es dem Benutzer vollkommen verborgen, wenn ein WWW-Server Informationen auf dem Benutzer-PC abgelegt hat. Erst die neueren Versionen von WWW-Browsern beinhalten Kontrollmöglichkeiten für den Benutzer, indem ihm eine Warnung bei einem Cookie-Zugriff angezeigt wird. Hier stellt man sehr schnell fest, daß sehr viele Anbieter die Server-Besuche quittieren. Diese Kontrollmöglichkeiten sollten unbedingt genutzt werden. Aber auch bei Verwendung älterer Versionen kann der Benutzer seine Spuren verringern, indem er entweder die Cookie-Datei gegen einen schreibenden Zugriff schützt oder regelmäßig löscht.

4.8.5 Videoüberwachung

Sowohl im öffentlichen als auch im privaten Bereich gewinnt der Einsatz von Videotechniken zu den verschiedensten Zwekken immer größere Bedeutung.

Grundsätzlich ist danach zu unterscheiden, ob es sich beim Einsatz von Videotechniken um eine reine *Augenblicksüberwachung ohne Aufzeichnung* handelt, oder ob gleichzeitig eine *Aufzeichnung der von der Videokamera erfaßten Geschehnisse* erfolgt. Während eine Überwachung ohne Aufzeichnung, wenn sie offensichtlich ist oder ausdrücklich darauf hingewiesen wird, im Sinne eines „verlängerten Auges“ in bestimmten Bereichen hinnehmbar erscheint, stellt die Aufzeichnung einen erheblichen Eingriff in die Persönlichkeitsrechte der Betroffenen dar.

Wo und in welchem Umfang sehen sich Bürgerinnen und Bürger in ihrem Umfeld mit Videoüberwachungstechniken konfrontiert, und wie sind derartige Maßnahmen aus datenschutzrechtlicher Sicht zu beurteilen?

Zum Schutz von *öffentlichen und privaten Einrichtungen und Gebäuden* werden Videokameras vorwiegend zur Beobachtung der *Eingangsbereiche* eingesetzt. Diese Kameras sind in den meisten Fällen derart offensichtlich angebracht, daß sich hier ein ausdrücklicher Hinweis auf eine Videoüberwachung erübrigt. Soweit keine Aufzeichnung erfolgt, sind diese im öffentlichen Interesse liegenden Überwachungsmaßnahmen unproblematisch. Sollte neben der reinen Beobachtung des Geschehens allerdings auch eine Aufzeichnung erfolgen, ist dies nur bei konkreten Anhaltspunkten für eine Gefahrenlage zulässig. An den Umgang mit dem gespeicherten Datenmaterial sind dabei hohe Anforderungen hinsichtlich der Zweckbindung zu stellen. So sind die verwendeten Datenträger unverzüglich zu löschen, wenn sich aus ihrem Inhalt keine Relevanz ergibt. Eine Weitergabe (Übermittlung) an andere Stellen ist auszuschließen.

Auch in *öffentlichen Verkehrsmitteln* und *Gaststätten* ist zunehmend der Einsatz von Videoüberwachungstechniken zu beobachten. In diesem Bereich mangelt es häufig an deutlichen Hinweisen, obwohl wegen der mittlerweile weit fortgeschrittene Miniaturisierung der Geräte nicht davon ausgegangen werden kann, daß die Videoüberwachung für die Fahrgäste in jedem Falle erkennbar ist. Das Fehlen solcher Hinweise ist auch deswegen nicht nachzuvollziehen, weil man dadurch immerhin Abschreckungseffekte bei mutmaßlichen Straftätern erzielen könnte. Soweit Aufzeichnungen erfolgen, ist für eine unverzügliche Löschung der Speichermedien zu sorgen, wenn der Zweck der Aufzeichnung erfüllt ist. Dies sollte durch eine automatisierte Technik unterstützt werden. Eine manuelle Löschsperre könnte dann lediglich bei einer gegebenen Gefahrenlage (z.B. Vandalismus, Bedrohungen) aktiviert werden.

Beim Einsatz der Videoüberwachung durch *Kreditinstitute* oder in *Parkhäusern* kommt neben der Abschreckung von möglichen Straftätern und der Sicherung von Beweismaterial für den Fall einer versuchten oder vollzogenen Straftat noch ein anderer nicht zu unterschätzender Aspekt zum Tragen. Hier kann eine Aufzeichnung sogar im Interesse der eigenen Sicherheit des Betroffenen sein, wenn er und das jeweils von der Kamera erfaßte Umfeld beobachtet und gespeichert wird. Insbesondere bei der Benutzung von Geldautomaten mit entwendeten und dann mißbräuchlich benutzten Kreditkarten hat sich dieses Verfahren bereits häufiger als hilfreich erwiesen. Aber auch hier ist die Information der Betroffenen unverzichtbar.

Selbst im häuslichen Umfeld ist mittlerweile eine Ausbreitung des Gebrauchs von Videoüberwachungseinrichtungen durch *Nachbarn* zu konstatieren. Solange sich die Nutzung dieser Technik auf die reine Beobachtung des Eingangsbereichs zur Wohnung, zur Garage bzw. zum Grundstück beschränkt, ohne daß Aufzeichnungen angefertigt werden, ist dies bei entsprechend deutlichen Hinweisen auf die installierten Kameras noch zu akzeptieren. Dies gilt insbesondere dann, wenn es sich bei dem Beobachtenden um eine Person handelt, für die eine normale Überwachung seines Umfelds durch eigenen Augenschein aufgrund von Behinderungen nicht oder nur erheblich eingeschränkt möglich ist. Eine völlig andere Qualität gewinnen diese Überwachungsmaßnahmen in den Fällen, in denen das Beobachtete auf entsprechenden Datenträgern aufgezeichnet wird. Hier ist in der Regel von einem erheblichen Eingriff in das informationelle Selbstbestimmungsrecht von durch diese Aufzeichnung erfaßten Personen auszugehen. Mangels eindeutiger spezialgesetzlicher Regelungen zur Datenerhebung in diesem Bereich kann sich eine Videoaufzeichnung lediglich auf die Einwilligung von Betroffenen stützen. Diese Einwilligung ist möglicherweise noch bei einem unmittelbar beteiligten Nachbarn zu erhalten, sicher aber nicht bei zufällig in das Visier der Kamera geratenen Personen. Wer sich in derartig gelagerten Fällen in der Wahrnehmung seines Persönlichkeitsrechts beeinträchtigt sieht, kann nach derzeitigem Recht nur die Unterlassung solcher ihn betreffender Aufzeichnungen fordern[146].

Auch zur *Überwachung von Mitarbeitern* im privaten und öffentlichen Bereich wird in sicherheitsrelevanten Bereichen in zunehmendem Maße von Videoüberwachung Gebrauch gemacht. Hier werden neben den allgemeinen Persönlichkeitsrechten auch arbeits- bzw. dienstrechtliche

[146] vgl. Urteil des BGH v. 25. April 1995 – VI 2 R 272/94 (KG), NJW 1995, S. 1955

Belange berührt. Der Umgang mit dem auf diese Weise gewonnenen Datenmaterial, insbesondere Aufbewahrung, Auswertung und Vernichtung (Löschung) sollte normenklar in entsprechenden Betriebs- oder Dienstvereinbarungen zwischen der Geschäftsführung bzw. der Dienststellenleitung und der zuständigen Personalvertretung unter Einbeziehung des betrieblichen bzw. behördlichen Datenschutzbeauftragten geregelt werden. Ist die Aktivierung der Videoaufzeichnung an vorgegebene Ausnahmezustände gekoppelt (z.B. an Signale von Bewegungsmeldern aus normalerweise unbesetzten Räumlichkeiten), so ist regelmäßig davon auszugehen, daß diese Aufzeichnung der Beweissicherung dient und entsprechend verwertet wird. Eine Beobachtung ohne Aufzeichnung kann bereits in solchen Fällen angezeigt sein, wenn sich in definierten Sicherheitsbereichen das Vier-Augen-Prinzip auf andere Weise nicht oder nur mit unvertretbarem personellem Aufwand durchsetzen läßt.

4.8.6 Zum täglichen Umgang mit der Informations- und Kommunikationstechnik

Obwohl die technische Entwicklung die Datenschutzbeauftragten und die informationstechnischen Sicherheitsfachleute immer wieder vor neue Herausforderungen stellt, um Sicherheit trotz oder mit Technik zu erzeugen, ist es der alltägliche und routinierte Umgang mit gewohnter Informations- und Kommunikationstechnik, der immer noch die meisten Risiken für den Datenschutz und die IT-Sicherheit erzeugt. Der alltägliche Trott führt aber häufig dazu, daß auch Fehler zur Routine werden: Paßwörter werden nicht geändert, leichtfertig ausgewählt oder offenbart, beim Faxgerät wird nicht mehr so genau hingesehen, welche Nummern man eigentlich wählt, beim PC meldet man sich nicht ab, wenn man den Arbeitsplatz verläßt, die Liste mit vertraulichen Daten verschwindet achtlos im Papierkorb. Warum sollte man auf diese Dinge auch achten, es ist ja noch nichts passiert ...

Wir wollen auch nicht, daß etwas passiert, wenn auch ein kleiner Vorfall mal eine heilsame Lehre sein kann. Ob es aber ein kleiner Vorfall ist, wenn sich ein leichtfertig in Kauf genommenes Risiko realisiert, oder ob es eine handfeste Havarie werden kann, die schwerwiegende Folgen nach sich zieht, ist meist eine Frage des Zufalls.

Um die Sicherheit der Verarbeitung und Datenschutz im Umgang mit Informationstechnik und -medien nicht dem Zufall zu überlassen, geben die Datenschutzbeauftragten auch Hinweise zu den einfachen Fragen des täglichen Datenschutzes.

Umgang mit Paßwörtern

Die meistverwendete Methode der Authentifikation eines Benutzers gegenüber einem IuK-System ist das Paßwort, mit dem dem System gegenüber der Nachweis erbracht werden kann, daß der Benutzer auch derjenige ist, als der er sich dem System gegenüber vorgestellt (identifiziert) hat. Der Benutzer authentifiziert sich mit einem Wissen, das er allen anderen Benutzern voraus hat: seinem persönlichen geheimen Paßwort.

Die Zuverlässigkeit der Authentifizierung steht und fällt mit der Geheimhaltung des Paßwortes. Wird es anderen Personen bekannt, können sie das System mit den Rechten des Betroffenen nutzen. Aber selbst die Kollegin oder der Kollege, die die gleiche Berechtigung haben, dürfen das Paßwort nicht kennen. Sie oder er könnten sonst Manipulationen an den Daten durchführen, die dann dem Betroffenen zugeordnet werden, für die sich also der Betroffene verantworten muß.

Hier gilt das unter Ziffer 4.8.3 Ausgeführte. Im Zusammenhang mit den bereits vom das IT-Grundschutzhandbuch erfaßten Maßnahmen sind weitergehende Empfehlungen zu prüfen und ggf. auf der Grundlage des Rahmenkonzeptes IT-Sicherheit in entsprechende ressortübergreifende Anforderungen an den IT-Einsatz umzusetzen.

Damit die Paßwörter möglichst geheim bleiben können, sind eine Vielzahl von Regeln von Benutzern und Systemverwaltern zu beachten und Anforderungen an die Technik und die Organisation zu stellen. Wir haben daher „Empfehlungen für die Vergabe von Paßwörtern“ formuliert[147].

Datenschutz und Telefax

Was alles mit Telefaxgeräten angestellt werden kann, ist mehrfach in früheren Jahresberichten behandelt worden[148]. Die Senatsverwaltung für Inneres hat unsere Ausführungen zum Anlaß genommen, in einem *Rundschreiben* nachdrücklich auf die Gemeinsame Geschäftsordnung hinzuweisen, die die Übertragung vertraulicher Schreiben mit Telefax auch in Eilfällen verbietet.

Dies führt natürlich nicht von heute auf morgen zur völligen Zurückhaltung beim Versand vertraulicher Dokumente per Telefax, dämmt aber die Häufung von „Unfällen“ bei der Fax-Übertragung ein. Selbstverständlich ist der leichtfertige Umgang mit Faxgeräten keine Berliner Besonderheit, sondern tritt in allen Bundesländern auf. Daher haben sich die Datenschutzbeauftragten des Bundes und der Länder in einer ausführlichen Presseerklärung dazu geäußert[149]. Neben den erneut wiederholten Hinweisen zur Sicherstellung der Vertraulichkeit der Faxsendungen bei der Übertragung und beim Empfang sowie zur korrekten Adressierung (Anwahl) der Kommunikationsverbindung wird auf einige Probleme hingewiesen, die mit dem Fortschritt der Telefaxtechnik verbunden sind:

Moderne konventionelle Telefaxgeräte ermöglichen die Fernwartung, ohne daß der Besitzer diese wahrnehmen kann. Seitenspeicher können so unbefugt gelesen, Rufnummern- und Parameterspeicher unbefugt gelesen und geändert werden.

Die Absendung von Dokumenten über Telefax erfolgt häufig direkt aus der Bürokommunikationsanlage des Absenders. Damit verbunden sind Risiken für die Vertraulichkeit der Sendungen, für die konkrete Anwahl und für die Sicherheit des Bürokommunikationssystems gegen Angriffe von außen über die Telekommunikationsschnittstelle.

5. Organisation des Datenschutzes

5.1 Sicherstellung des Datenschutzes

5.1.1 Betriebliche und behördliche Datenschutzbeauftragte

Im abgelaufenen Jahr gab es in der öffentlichen Verwaltung zum ersten Mal Fälle, bei denen die gesetzlich vorgeschriebene *Unabhängigkeit der behördlichen Datenschutzbeauftragten* in Frage gestellt wurde.

Die Leitung einer großen öffentlichen Einrichtung faßte in einer ihrer turnusmäßigen Sitzungen den Beschluß, den nebenamtlichen behördlichen Datenschutzbeauftragten gegen seinen Willen *abzuberufen*. Im wesentlichen wurden seine Leistungen für den Teil seiner Arbeit beanstandet , der sein eigentliches Aufgabengebiet betraf und in dem er überwiegend beschäftigt war. Die Tätigkeit als behördlicher Datenschutzbeauftragter, für die ihm lediglich ein Fünftel seiner Arbeitszeit zugestanden wurde, wurde nicht geprüft.

Die Abberufung sollte nicht als Sanktionsmaßnahme gegen

[147] vgl. Anlage 6.1
[148] JB 1994, 3.5: „Telefax – eine Pannengeschichte“
[149] vgl. Anlage 6.2

den behördlichen Datenschutzbeauftragten betrachtet werden, sondern vielmehr aus Gründen der Fürsorgepflicht einen Beitrag dazu leisten, daß der Betroffene seine Aufgabe, für die er eigentlich eingestellt war, wieder voll erfüllen kann. Die Leitung des Hauses bat den Berliner Datenschutzbeauftragten gem. § 36 Abs. 3 BDSG um Zustimmung zu der beabsichtigten Maßnahme. Gleichzeitig wurde uns mitgeteilt, daß in der gleichen Sitzung ein neuer behördlicher Datenschutzbeauftragter bestellt wurde.

Eine vorzeitige Beendigung der Tätigkeit des behördlichen Datenschutzbeauftragte ist nur über zwei Wege erreichbar. Entweder muß ein *Abberufungsverlangen der Aufsichtsbehörde* nach

§ 38 Abs. 5 Satz 3 BDSG vorliegen, oder die speichernde Stelle muß in entsprechender Anwendung des § 626 BGB eine *Kündigung* aussprechen.

Voraussetzung für die erste Alternative ist nach § 38 BDSG jedoch die mangelnde Fachkunde oder Zuverlässigkeit oder offensichtliche Inkompatibilität für die Erfüllung der dem behördlichen Datenschutzbeauftragten übertragenen Aufgaben (förmliches Abberufungsverfahren). Eine solche mangelnde Qualifikation, Zuverlässigkeit oder Unvereinbarkeit mit dem Amt konnte jedoch von uns nicht festgestellt werden, da der Betroffene uns als engagierter behördlicher Datenschutzbeauftragter bekannt war.

Die datenverarbeitende Stelle konnte die Bestellung des Datenschutzbeauftragten nur bei Anwendung von § 626 BGB widerrufen, wozu ein wichtiger Grund vorliegen muß. Dieser würde vorliegen, wenn der behördliche Datenschutzbeauftragte beharrlich untätig wäre, einen schwerwiegenden Verstoß gegen seine Verschwiegenheitspflicht begehen oder sich eines Vergehens gegen eine einschlägige Vorschrift (z.B. §§ 201 ff. StGB, § 43 BDSG) schuldig machen würde. Auch dies war nicht der Fall.

Wir sahen uns daher nicht in der Lage, der Bitte zu entsprechen und die Abberufung des behördlichen Datenschutzbeauftragten zu verlangen.

In einem zweiten Fall hatte die Dienststelle ebenfalls die Absicht, den behördlichen Datenschutzbeauftragten von seinem Amt zu entbinden. Begründet wurde dies damit, daß die Rechtsabteilung, der der Datenschutzbeauftragte organisatorisch angehörte, im Rahmen der *Senatsumbildung* zusätzliche Aufgaben erhalten hatte, ohne personelle Entlastungen zu erfahren. Dies wollte man damit kompensieren, daß der behördliche Datenschutzbeauftragte wieder voll seine eigentlichen Aufgaben in der Rechtsabteilung übernehmen sollte. Das Amt sollte zwar von einem anderen Mitarbeiter weiterhin ausgeübt werden, doch war der behördliche Datenschutzbeauftragte nicht bereit, sein Amt freiwillig aufzugeben.

Wie im ersten Fall ist eine Abberufung des behördlichen Datenschutzbeauftragten gem. § 19 Abs. 5 BlnDSG i.V.m. § 36 Abs. 3 Nr. 4 BDSG nur möglich, wenn die Aufsichtsbehörde es verlangt oder § 626 BGB zur Anwendung kommt.

Beide Voraussetzungen waren auch hier nicht gegeben. Wir haben dem behördlichen Datenschutzbeauftragten unsere Unterstützung zugesagt, vor allem vor dem Hintergrund, daß er sich bei früheren Gelegenheiten über mangelnde Unterstützung in seinem Hause beklagt hatte und nun die Vermutung nahelag, daß man sich eines unbequemen Sachverwalters des Datenschutzes entledigen wollte.

Die Fälle zeigen, daß die verbreitet geübte Praxis, irgend jemanden zum behördlichen Datenschutzbeauftragten zu benen-

nen, für die datenverarbeitenden Stellen zu häufig unvermuteten Konsequenzen führt. Die Bestellung eines behördlichen Datenschutzbeauftragten mag noch nach Belieben erfolgen. Dies gilt jedoch keineswegs für seine Abberufung, falls er nicht selbst damit einverstanden ist.

5.1.2 Dateienregister

Viele datenverarbeitende Stellen des Landes haben nach wie vor Probleme damit, Meldungen zum Dateien- und Geräteverzeichnis nach § 25 BlnDSG in der von der *Dateiregisterordnung* vorgesehenen Form aufzuliefern und den Meldestand aktuell zu halten. Neben den Stellen, die routinemäßig ihrer Meldepflicht nachkommen, weil sie sich organisatorisch auf die gesetzliche Verpflichtung zur Führung einer internen Übersicht über die eigenen Dateien mit personenbezogenen Daten und die eingesetzten Geräte eingestellt haben, gibt es Stellen, die offensichtlich damit überfordert sind, der Meldepflicht in rechtmäßiger Form nachzukommen, und nicht wenige, die die Umsetzung dieser bindenden Rechtsvorschrift boykottieren. Dies gilt vor allem für eine Reihe von Bezirksämtern, insbesondere im Zusammenhang mit dem Geräteverzeichnis. Der Zweck des Dateienregisters kann damit nicht erfüllt werden.

Typisch für den Unwillen vieler Behörden, ihrer Meldepflicht nachzukommen, ist die Suche nach *Ausnahmeregelungen*, die von der Meldepflicht befreien. Darunter fallen Dateien, die vom Berliner *Informationsverarbeitungsgesetz (*IVG) erfaßt werden, weil sie bei der allgemeinen Verwaltungstätigkeit benutzt werden, also der „Verwaltung der Verwaltung“ dienen. Weiter fallen darunter jene Dateien, die nur zeitweise aus *verarbeitungstechnischen Gründen* entstehen (§ 19 Abs. 3 BlnDSG). Ferner gibt es natürlich keine Meldepflicht, wenn die Dateien nicht personenbezogen sind.

Zwei Fälle zeigen die Probleme damit auf:

Eine *anerkannte Privatschule* fragte an, ob personenbezogene Daten von *Bewerbern*, die ein Auswahlverfahren durchlaufen, unter die Bestimmungen des IVG fallen und somit nicht gemeldet werden müssen. In der Schuldatenverordnung findet sich jedoch eine explizite Rechtsgrundlage für die Speicherung der fraglichen Daten. Es ist auch geregelt, daß für den Fall, daß Bewerber nicht angenommen werden, die Daten nach sechs Monaten zu löschen sind. Das IVG gilt aber nur für solche Daten, für die es keine besonderen rechtlichen Vorschriften gibt (§ 1 Abs. 1).

In einem anderen Fall bat uns die Senatsverwaltung für Justiz um Stellungnahme zu der Auffassung einer Gerichtspräsidentin, daß die von *Richtern* auf ihren *privaten Rechnern* geführten Dateien und die dafür genutzten Geräte nicht zu melden seien, weil diese Daten nur vorübergehend gespeichert und verarbeitet werden. Die Daten würden nach Abschluß des Verfahrens wieder gelöscht oder anonymisiert werden.

Gem. § 22 Abs. 1 Satz 3 Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG) haben Richter usw. eine Meldung nach § 25 BlnDSG vorzunehmen, wenn sie personenbezogene Daten zur Unterstützung ihrer Tätigkeit auf eigenen Geräten verarbeiten. Diese Datenverarbeitung darf sich gem. § 22 Abs. 2 AGGVG nur auf laufende Verfahren beziehen. Danach sind die Daten zu löschen oder zu anonymisieren.

Aus dem datenschutzrechtlichen Grundprinzip, daß Daten zu löschen oder zu sperren oder alternativ zu anonymisieren sind, wenn sie für die Aufgabenerfüllung nicht mehr erforderlich sind, ergibt sich jedoch nicht, daß sie im Sinne von § 19 Abs. 3 BlnDSG temporär wären. Mit diesem Argument wären dann

Der Senat teilt die Auffassung des Berliner Datenschutzbeauftragten, daß die von Richtern auf ihren privaten Rechnern geführten Dateien und die dafür genutzten Geräte zum Dateienregister zu melden sind, wenn personenbezogene Daten auf eigenen Geräten verarbeitet werden. Die insoweit zuständige Senatsverwaltung für Justiz hat die anfragende Gerichtspräsidentin angewiesen, für entsprechende Meldungen Sorge zu tragen.

alle personenbezogenen Daten temporär, denn sie werden nur für einen endlichen Zeitabschnitt vorgehalten.

Dateien sind gem. § 19 Abs. 3 BlnDSG hinsichtlich der Meldepflicht nur privilegiert, wenn sie bei der automatischen Verarbeitung ausschließlich aus verarbeitungstechnischen Gründen vorübergehend gehalten werden. Dabei handelt es sich um personenbezogene Dateien, die im Rahmen der Arbeitsabläufe bei der Verarbeitung personenbezogener Daten zeitweilig entstehen, ohne daß sie einem anderen Zweck dienen würden, etwa Zwischenergebnisse eines Datenverarbeitungsprozesses, die je nach Art des Prozesses für Tage (z.B. Batch-Prozesse) oder auch nur Bruchteile von Sekunden (z.B. temporäre Zwischentabellen bei Abläufen in relationalen Datenbanksystemen) bestehen.

Ein Datenbestand, der Nachnamen von Klägern, Aktenzeichen und Streitgegenstände enthält, ist auch nicht anonym. Schon diese drei Angaben an sich weisen eindeutigen Personenbezug auf, insbesondere, wenn der Nachname selten genug auftritt. Für einen Richter, der sich mit einem Urteil oder Beschluß befaßt hat, dürfte die Zuordnung zu einer ihm bekanntgewordenen Person selbstverständlich möglich sein. Selbst wenn es Aufwand für einen Richter bedeutet, entsprechende Verfahrensakten beizuziehen, so kann der Personenbezug ohne weiteres über diese Akten wieder hergestellt werden, sei es durch Einschaltung von Zugriffsberechtigten oder durch nicht legales Handeln.

Die Schwierigkeiten mit dem Dateienregister sowie der Aufwand für die Führung der Register beim Datenschutzbeauftragten könnten Anlaß für eine Prüfung sein, ob nicht im Rahmen der Umsetzung der EU-Richtlinie von der Möglichkeit Gebrauch gemacht werden sollte, die Register zugunsten der Führung interner, selbstorganisierter Verzeichnisse abzuschaffen (Art. 18 Abs. 2).

Die Anregung des Berliner Datenschutzbeauftragten wird bei einer möglichen Novellierung des Berliner Datenschutzgesetzes im Rahmen der Umsetzung der EU-Richtlinie geprüft.

5.2 Der Berliner Datenschutzbeauftragte

5.2.1 Die Dienststelle

Ende Juli 1996 ging der Bereichsleiter für Private Datenverarbeitung, Senatsrat Dr. Dieter Baumeister, in den Ruhestand. Ein Jahr zuvor war er im Zusammenhang mit der Übernahme der Aufgaben der Aufsichtsbehörde von der Senatsverwaltung für Inneres in unsere Dienststelle versetzt worden. Dort hatte er viele Jahre das für Datenschutz zuständige Referat geleitet und war maßgeblich an der Entstehung des Berliner Datenschutzgesetzes beteiligt. Die damit verbundenen Personalveränderungen wurden zum Anlaß genommen, die Zuständigkeiten in der Dienststelle neu zu verteilen[150]. Die grundlegende Idee dabei war, soweit wie möglich zusammengehörige Bereiche unabhängig davon, ob es sich um private oder öffentliche Stellen handelt, zusammenzuführen. Die für die neu entstandenen Arbeitsgebiete zuständigen Referenten nehmen nunmehr ihre Aufgaben gleichermaßen für Behörden und Privatunternehmen wahr. Dies entspricht sowohl der Erwartung der Bürger, die z.B. eine Gleichbehandlung des Datenschutzes in öffentlichen und privaten Krankenhäusern erwarten, als auch den Vorgaben der europäischen Datenschutzrichtlinie, die von einer grundsätzlichen Gleichstellung des öffentlichen und privaten Sektors ausgeht[151]. Nach dem Scheitern der Fusion mit Brandenburg bleiben die Aufgaben der Dienststelle zwar weiterhin auf Berlin beschränkt. Es zeichnet sich allerdings ab, daß es zur weiteren Gründung gemeinsamer Einrichtungen beider Länder kommen wird; auch eine Vielzahl gemeinsamer

[150] vgl. die neue Geschäftsverteilung in Anlage 7
[151] vgl. JB 1995, 1.2

Datenverarbeitungsverfahren wird entstehen. Dies wird eine verstärkte Zusammenarbeit mit dem Brandenburgischen Landesbeauftragten für den Datenschutz erforderlich machen, die auch in gemeinsamen Besprechungen schon vorbereitet wurde.

5.2.2 Aufgabenentwicklung

Während die Zahl der Eingaben im öffentlichen Bereich in etwa gleichgeblieben ist, gab es erneut einen starken Anstieg von Beschwerden über Privatunternehmen. Dies ist sicherlich darauf zurückzuführen, daß die Übertragung der Aufgaben der Aufsichtsbehörde auf den Datenschutzbeauftragten zu einer besseren Wahrnehmung der datenschutzrechtlichen Probleme im Alltag geführt hat. Auch die Amtsüberprüfungen bei Unternehmen, die Daten für fremde Zwecke verarbeiten (Auskunfteien und Detekteien, Adressenhandel, Aktenvernichtungsunternehmen u.ä.) wurden wieder aufgenommen.

Die meisten Beschwerden im öffentlichen Bereich waren in diesem Jahr im Arbeitsgebiet Polizei zu bearbeiten, gefolgt von der Justiz. Die 1995 beobachtete hohe Anzahl von Beschwerden im Ordnungsbereich, insbesondere im Meldewesen, stand offensichtlich im Zusammenhang mit den Wahlen und ging wieder deutlich zurück. Bei den Beratungsersuchen dominierten erneut die Arbeitsgebiete Schule, Wissenschaft und Forschung einerseits und Gesundheit und Soziales andererseits. Man kann hieran deutlich erkennen, daß die klassischen Eingriffsverwaltungen eher reaktiv tätig werden, während in den Leistungsverwaltungen das Interesse an frühzeitiger Beratung deutlich höher ist. Im privaten Bereich ist es naturgemäß zu einem Rückgang von Beschwerden über die BahnCard[152] gekommen, dafür stiegen die Beschwerden von Mietern gegen ihre Vermieter deutlich an. Auffällig ist auch die Anzahl von Eingaben gegen Ärzte und Krankenhäuser sowie Beschwerden über den Umgang mit Personaldaten.

Bei den technischen Prüfungen kam es im Zusammenhang mit unseren Aktivitäten gegenüber Privatunternehmen zu einem deutlichen Anstieg des PC–Anteils gegenüber anderen Verfahren[153]. Dies liegt daran, daß der PC zumindest im Bereich der kleineren und mittleren Betriebe das zentrale Organisationsmittel ist. In der öffentlichen Verwaltung lag dagegen der Schwerpunkt auf der Beratung der Großverfahren, deren Einsatz im vergangenen Jahr gestartet oder vorbereitet wurde[154].

Eine flächendeckende Prüfung und Beratung der luK-Verfahren in unserem Zuständigkeitsbereich ist allerdings völlig ausgeschlossen. Nach der letzten Statistik der Industrie- und Handelskammer gibt es in Berlin ca. 125 000 Gewerbetreibende und ca. 80 000 Kleingewerbe und freie Berufe; bei allen ist davon auszugehen, daß sie Informationstechnik verwenden. In der Hauptverwaltung und den Bezirksämtern existieren nach den letzten Angaben im Abgeordnetenhaus-Informationssystem (AIS) vom März 1996 alleine über 23 000 Bildschirmarbeitsplätze; zum gleichen Zeitpunkt waren 225 Großrechner gemeldet. Nicht darin enthalten sind die selbständigen Körperschaften und Anstalten; insbesondere die Berliner Hochschulen verfügen über immense Rechnernetze, deren Kontrolle allein mehr Kapazitäten verschlingen würde als uns an Dienstkräften zur Verfügung steht: Im Bereich Informatik sind das je ein Mitarbeiter bzw. eine Mitarbeiterin für Großrechner, für Kommunikationssysteme, für Personalcomputer und für Client-

[152] vgl. JB 1995, 3. 1
[153] vgl. oben 4.8.3
[154] vgl. z.B. oben 4.1.1, 4.2.1, 4.8. 1

Server-Architekturen.

Eine andere Zahl aus dem AIS ist vielleicht auch von Interesse: Für den Datenschutzbeauftragten gibt jeder Bürger Berlins jährlich 1 DM aus, für luK allein für Hauptverwaltung und Bezirksämter 66 DM; auch hier sind Körperschaften und Anstalten nicht enthalten. Mit dieser einen DM sind auch die Kontrollen in der gesamten Privatwirtschaft finanziert.

Einen nicht unerheblichen Anteil an der Arbeit machen die *Vortragstätigkeit* sowie die Beteiligung an *Aus- und Fortbildung* aus. Eine Reihe von Mitarbeitern zeigte weit über die Arbeitszeit hinaus erneut ihr Engagement, bei Konferenzen und Kongressen, in Schulen und Hochschulen oder in Verbänden und Interessenvereinigungen Kenntnisse über den Datenschutz zu vermitteln und sich an den Diskussionen über die Fortentwicklung des Datenschutzes zu beteiligen.

5.2.3 Umgang mit dem Datenschutzbeauftragten

Bereits im vergangenen Jahr wurde auf Probleme *mangelnder Unterstützung des Datenschutzbeauftragten* hingewiesen[155]. In der letzten Zeit ist bei Teilen der Berliner Verwaltung die Tendenz zu beobachten, Probleme des Datenschutzes nicht nur zu vernachlässigen, sondern die Arbeit des Datenschutzbeauftragten zu behindern. Unliebsame Anfragen werden nicht oder nur mit großem Zeitverzug bearbeitet, die Zuständigkeit des Datenschutzbeauftragten wird aus unzutreffenden Gründen bestritten oder es wird gar offen erklärt, man lehne es ab, die gegebene Rechtslage zu berücksichtigen. Über zwei Fälle wurde oben berichtet[156].

Für die zögerliche Bearbeitung ein Beispiel: Im Jahresbericht 1995 hatten wir auf Datenschutzprobleme im Zusammenhang mit der *Einbürgerung* hingewiesen[157]; dies ging auf eine Beanstandung zurück, die im Januar dieses Jahres ausgesprochen worden war. Nachdem im Juli 1995 wegen Organisations- und Strukturaufgaben um Fristverlängerung gebeten worden war, wurde im September 1995 die Ausarbeitung neuer Formulare angekündigt. Im Februar 1996 erfolgte ein erneuter Hinweis auf „Aufgabenerledigungsschwierigkeiten“, ansonsten erhielten wir bis Ende 1996 trotz mehrfacher Mahnung auch beim Abteilungsleiter keine Reaktion mehr. Erst im Laufe der späteren Beratungen im Unterausschuß „Datenschutz“ erfolgte gegenüber dem Parlament eine Stellungnahme und eine Entschuldigung für die Verzögerung. Erstaunt stellten wir fest, daß im Laufe des Jahres 1996 einige Verfahrensänderungen vorgenommen worden waren; uns hierüber zu informieren, hielt man nicht für nötig.

Derartige Bearbeitungszeiten kommen zunehmend häufiger vor. Dies verzögert nicht nur die Aufklärung, ob die Praxis datenschutzgerecht ist oder rechtsfehlerhaft arbeitet, sondern wird auch dem Anspruch der Bürger auf zügige Bearbeitung ihrer Anliegen nicht gerecht.

5.2.4 Zusammenarbeit mit dem Abgeordnetenhaus

Die neue Berliner Verfassung siedelt den Datenschutzbeauftragten bei den Bestimmungen zur Volksvertretung an (Artikel 47). Er ist zwar eigene Oberste Landesbehörde, hat jedoch aufgrund dieser Stellung gegenüber dem Abgeordnetenhaus besondere Rechte und Pflichten[158]. Auch im Berichtsjahr hat er anläßlich der Einbringung des Jahresberichts 1995 sowie der Senats-

Die im Jahresbericht 1995 erhobenen Beanstandungen wurden von der zuständigen Senatsverwaltung selbstverständlich sämtlich aufgegriffen und geprüft. Wegen der Vielzahl der zu beteiligenden Behörden und der teilweise notwendigen Abstimmungen mit anderen Bundesländern – handelt es sich bei den Beanstandungen zugrundeliegenden Rechtsmaterie doch um einheitlich anzuwendendes Bundesrecht – konnte eine sicherlich wünschenswerte schnellere Bearbeitung nicht erreicht werden. Der Berliner Datenschutzbeauftragte ist von der zuständigen Senatsverwaltung darüber regelmäßig in Kenntnis gesetzt worden.

[155] JB 1995, 7.1
[156] vgl. oben 4.1.2, 4.4.4
[157] JB 1995, 5.5.3
[158] §§ 22 Abs. 4, 29 BlnDSG

stellungnahme hierzu im Plenum des Abgeordnetenhauses eine kurze *Rede* gehalten, in der er bereits auf die Schwierigkeiten einiger Teile der Verwaltung mit dem Datenschutz einging[159].

Am 24. September 1996 konstituierte sich der Unterausschuß „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung unter dessen Vorsitzenden Rüdiger Jakesch neu. Er nahm sofort die Beratungen zum Jahresbericht 1995 auf; daneben wurden Gesetzgebungsvorhaben und aktuelle Probleme erörtert. Auch in einer Reihe anderer Ausschüsse wurden Datenschutzprobleme unter unserer Beteiligung erörtert und unser Rat erfragt, unter anderem wiederum vom Petitionsausschuß. Die Zusammenarbeit mit den Fraktionen und einzelnen Abgeordneten wurde in der üblichen konstruktiven Weise auch im neuen Abgeordnetenhaus fortgeführt.

5.2.5 Kooperation mit Stellen außerhalb Berlins

Das Datenschutzgesetz verpflichtet den Datenschutzbeauftragten, mit allen Stellen zusammenzuarbeiten, die wie er die Aufgabe haben, die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren (24 Abs. 4 BlnDSG). Die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* ist hierfür das wichtigste Gremium. Sie tagte unter Vorsitz des Hamburgischen Datenschutzbeauftragten im Berichtsjahr zweimal; die dort gefaßten Beschlüsse sind im Anhang abgedruckt[160]. Von großer Bedeutung sind die im Rahmen der Konferenz gebildeten Arbeitskreise, da der dort stattfindende Erfahrungsaustausch ein notwendiges Mittel ist, den in den kleinen Dienststellen vorhandenen Sachverstand zu verbreitern und die vorhandenen bescheidenen Kräfte zu bündeln. Den Vorsitz im Arbeitskreis Medien führt seit Anfang an Berlin; in mehreren Sitzungen, bei denen auch ein intensiver Erfahrungsaustausch mit den Anbietern von Online-Diensten stattfand, wurde nach gemeinsamen Lösungen gesucht und entsprechende Konferenzbeschlüsse vorbereitet. Auch bilateral wurde eine Vielzahl von Kooperationsgesprächen mit dem Bundes- und anderen Landesbeauftragten geführt, besonders mit dem Brandenburgischen Landesbeauftragten.

Auch die Kooperation mit den Obersten Aufsichtsbehörden der Länder im *„Düsseldorfer Kreis“* und mit dessen Arbeitskreisen wurde fortgeführt. Für den Bereich der Sparkassen haben wir eine Vermittlerfunktion zwischen diesem Gremium und der Konferenz übernommen, um eine gleiche Bewertung bei öffentlichen und privaten Kreditinstituten zu gewährleisten. In Berlin wurde auch ein Dialog von Bundes- und Landesbeauftragten, Aufsichtsbehörden und Rundfunkdatenschutzbeauftragten zur Gewährleistung einer einheitlichen Prüfpraxis bei den Neuen Medien aufgenommen, der allerdings wegen der zögerlichen Haltung der meisten Aufsichtsbehörden vorläufig noch nicht fortgeführt werden konnte.

Auf *internationaler Ebene* beteiligten wir uns an den Aktivitäten der Internationalen Konferenz der Datenschutzbeauftragten und der Konferenz der Datenschutzbeauftragten der EU. Besonderes Schwergewicht lag für uns wie im nationalen Bereich wiederum auf Problemen des Datenschutzes bei der Telekommunikation. Die Arbeitsgruppe Telekommunikation im Rahmen der Internationalen Konferenz tagte zweimal und befaßte sich insbesondere mit Problemen des Datenschutzes im Internet[161].

[159] vgl. Anlage 1
[160] vgl. Anlagen zu 2
[161] vgl. oben 4.7.1; Anlage 5.1

Auf europäischer Ebene engagierten wir uns im Verfahren zur Verabschiedung der ISDN-Richtlinie[162]; eine besondere Koordination mit der von der französischen Datenschutzkommission geleiteten europäischen Arbeitsgruppe zu internationalen Datennetzen wurde vereinbart.

5.2.6 Öffentlichkeitsarbeit

Zur Konsolidierung der angespannten Haushaltslage, in der sich das Land Berlin befindet, sind Einsparungen in allen Bereichen der öffentlichen Verwaltung unumgänglich. Auch die Mittel für unsere Öffentlichkeitsarbeit sind davon nicht ausgenommen. Dem steht das immense Interesse der Bürger an sachbezogenen und verständlichen Informationen zu datenschutzrechtlichen Fragestellungen entgegen. Wir haben versucht, beiden Anliegen gerecht zu werden.

In unserer Reihe „Materialien zum Datenschutz“ sind zwei neue Hefte erschienen. In der Broschüre „*Medien und Persönlichkeitsschutz* – Materialien 23 zum Datenschutz“ sind Dokumente veröffentlicht, die sich mit den neuen Herausforderungen und Möglichkeiten im Medienbereich – z.B. durch neue Formen des elektronischen Publizierens, Öffnung der Medienarchive und Pressedatenbanken und den Ausbau neuer digitaler Kommunikationsformen (z.B. Video on demand) – und den damit verbundenen Auswirkungen auf die Persönlichkeitsrechte des Einzelnen befassen. Personenbezogene Daten werden in immer größerem Umfang weltweit verarbeitet und ausgetauscht. Die sich daraus ergebenden Risiken für die Privatsphäre des Einzelnen und den Datenschutz können deshalb nur weltweit begrenzt werden. Mit dem Heft „*Internationaler und Europäischer Datenschutz* – International and European Data Protection – Materialien 24 zum Datenschutz“ wollen wir auf diesen Umstand hinweisen. In der – zweisprachigen (deutsch/englisch) – Broschüre sind erstmals die internationalen und europäischen Richtlinien und Konventionen zum Datenschutz veröffentlicht. Außerdem sind Dokumente aus den Vereinigten Staaten von Amerika und aus der Russischen Föderation enthalten.

Wie adressiere ich ein Schreiben, das ungeöffnet einen Sachbearbeiter erreichen soll? Wie läuft die Postverteilung in Behörden? Werden die Briefe zentral geöffnet und dann offen weitergeleitet? Diese und andere Fragen zum Schriftwechsel mit Behörden werden vielfach an uns herangetragen. Unser *Faltblatt „Datenschutz INFO 1 – Wie schreibe ich an Behörden?“* ist die Antwort auf diese Fragen. Es wird das Postverteilungsverfahren bei Behörden dargestellt und anhand von Beispielen gezeigt, wie durch bestimmte Adressierungen sichergestellt wird, daß Schreiben offen oder verschlossen an eine bestimmte Person gelangen. Die geplante Herausgabe weiterer Datenschutz-INFOs scheiterte an der Haushaltslage.

Neben den vorstehend genannten Veröffentlichungen ist über zwei weitere Schwerpunkte in der Öffentlichkeitsarbeit zu berichten:

Im Berichtsjahr haben wir ein neukonzipiertes *Datenscheckheft* herausgebracht. Dieses inzwischen über zehn Jahre alte Informationsmaterial, das auch von anderen Datenschutzbeauftragten übernommen wurde und bundesweit bekanntgeworden ist, ist bei den Bürgern wegen seines praktischen Ansatzes sehr beliebt. Auch das neue Datenscheckheft wurde uns wieder förmlich „aus den Händen gerissen“. Es ist daher ebenfalls schon wieder vergriffen und konnte bislang nicht nachgedruckt werden.

[162] vgl. oben 4.7.1

Ob Telekom, Ämter oder Adressenverleger – alle wollen erstmal nur das eine: Daten, Daten, Daten. Ohne sie können kein Antrag bearbeitet, kein Bußgeldbescheid erlassen, keine Gebühren eingetrieben und auch kein Werbebrief versandt werden.

Wie aber kann ich Auskunft über meine gespeicherten Daten erhalten? Bei welchen Stellen kann ich diese beantragen? Wie kann ich Akteneinsicht in über mich vorhandene Unterlagen bekommen? Wie die Berichtigung und Löschung meiner Daten erreichen?

Das neugestaltete Datenscheckheft bietet praktische Hilfe. Eine kleine Mappe enthält Kärtchen mit Informationen darüber, wer welche persönlichen Daten gespeichert haben könnte und auf welcher Rechtsgrundlage dies geschieht. 37 Musterbriefe helfen, den richtigen, aber auch rechtlich korrekten Ton zu finden, um den solcherart angeschriebenen Unternehmen, Verbänden oder Ämtern deutlich zu machen, was man will: Auskünfte über gespeicherte Daten, vorhandene berichtigen, andere löschen. Enthalten sind beispielsweise Schreiben, mit denen die Zusendung von Werbematerial unterbunden werden kann, sowie solche, mittels derer Auskunft und Akteneinsicht bei Polizei, Verfassungsschutz, Krankenkasse, Ärzten, Sozialämtern oder der SCHUFA beantragt werden kann. Die Musterbriefe können sogleich ausgefüllt und umgehend in einem Fensterumschlag verschickt werden.

Der Berliner Datenschutzbeauftragte im Internet

Seit dem 21.März 1996 ist der Berliner Datenschutzbeauftragte mit einem eigenen Programmangebot im Internet präsent.

Unter *http://www.datenschutz-berlin.de* sind vielfältige Informationen über den Datenschutz abrufbar. Ein Programmschwerpunkt ist die Vorstellung des jeweils aktuellen Jahresberichtes sowie die Bereitstellung der wesentlichen, darin zitierten Dokumente. Informationen über nationale und internationale Themen werden ebenfalls angeboten. In einer Übersicht werden die von uns herausgegebenen Broschüren und Materialien vorgestellt und können bei Bedarf abgerufen werden. Praktische Hinweise zur Selbsthilfe (z.B. im Umgang mit Behörden) werden unter dem Programmpunkt „Service“ bereitgestellt.

Das Angebot wird weltweit genutzt. Dies ist an den Anfragen erkennbar, die wir über e-mail erhalten[163]. Die (anonyme) Protokollierung im Server verzeichnete im Laufe des Jahres monatlich bis zu über 40 000 Abrufe, wobei die dabei nicht registrierten Abrufe auf „Proxyservern“ die Universitäten eingerichtet sind, nicht erfaßt werden.

Berlin, 4. März 1997

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

Berlin, den 27. Mai 1997

Der Senat von Berlin

Diepgen

Regierender Bürgermeister

[163] Unsere e-mail-Adresse lautet: mailbox@datenschutz-berlin.de