Bericht

des Berliner Beauftragten für Datenschutz und Akteneinsicht
zum 31. Dezember 1999

Der Berliner Beauftragte für den Datenschutz und das Recht auf Akteneinsicht hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am 17. März 1999 vorgelegten Jahresbericht 1998 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 1999 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Anlagenband („Dokumente zum Datenschutz 1999") veröffentlicht, der gemeinsam mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg herausgegeben wird.

Dieser Jahresbericht ist über das Internet ***(http://www.datenschutz-berlin.de)*** *abrufbar; wir bemühen uns, dort alle im Bericht zitierten Fundstellen zugänglich zu machen.*

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Akteneinsicht
Pallasstraße 25/26
10781 Berlin

Telefon: (0 30) + 78 76 88 44
Telefax: (0 30) 2 16 99 27
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Layout: Volker Brozio

Redaktion: Laima Nicolaus

Druck: Verwaltungsdruckerei Berlin

Die Broschüre wurde auf Umwelt-Recycling-Papier gedruckt!

Inhaltsverzeichnis

Anlagen zum Jahresbericht 1999

1. Rechtliche Rahmenbedingungen

1.1 Europa und Deutschland

Auch der neuen Bundesregierung ist es bisher nicht gelungen, einen endgültigen Entwurf für die richtlinienkonforme Anpassung des *Bundesdatenschutzgesetzes* (BDSG) an die *Europäische Datenschutzrichtlinie* (EU-Richtlinie) vorzulegen[1]. Die Folge ist, dass die Europäische Kommission im vergangenen Jahr bereits zwei „blaue Briefe" an die Bundesregierung geschickt hat und eine Klage beim Europäischen Gerichtshof vorbereitet[2].

Eine der wesentlichen Ursachen der Verzögerung ist ein Dilemma, in dem sich die Bundesregierung befindet. Einerseits ist allen Beteiligten klar, dass der von der vorherigen Regierung übernommene Entwurf die Vorgaben der Richtlinie nicht hinreichend umsetzte, technologiepolitische Akzente vermissen ließ und dabei so kompliziert war, dass selbst Fachleute Schwierigkeiten haben, die einzelnen Regelungen nachzuvollziehen. Von daher wäre es erforderlich gewesen, eine völlig neue Konzeption des deutschen Datenschutzrechts ins Auge zu fassen, die Richtlinienkonformität, Zukunftsgerichtetheit und Verständlichkeit in sich vereinigt. Die Entwicklung eines derartigen Konzepts würde allerdings so lange dauern, dass von den europäischen Behörden nicht unerhebliche Sanktionen verhängt würden – ungeachtet des Umstands, dass ein Rechtszustand, der mit den europäischen Vorgaben nicht zu vereinbaren ist, nicht zufrieden stellen kann und es wegen der nach Ablauf der Umsetzungsfrist geltenden unmittelbaren Wirkungen[3] zu erheblichen Anwendungsschwierigkeiten insbesondere beim grenzüberschreitenden Datenverkehr kommt[4]. Um dies zu verhindern, blieb kein anderer Weg, als auf der Basis der übernommenen Vorarbeiten einen Gesetzesentwurf zu entwickeln, der die bislang nicht enthaltenen unerlässlichen Regelungen enthält und gewisse Impulse für die Fortentwicklung der Datenschutztechnik gibt (z. B. Verankerung des Datensparsamkeitsprinzips, Regelungen zur Chipkarte und zur Videotechnik). Der auf dieser Basis im Sommer vorgelegte neue Vorentwurf[5] wurde in den letzten Monaten des Jahres intensiv diskutiert. Die von mehreren Seiten erhobenen Einwände führten immer wieder zur Verzögerung bei der Fertigung der endgültigen Kabinettsvorlage, die bis in das neue Jahr hineinreichten. Vor allem eine öffentliche Initiative des Deutschen Presserates hemmte die Arbeiten. Aufgrund einer überzogenen Fehl-

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABlEG L 281/31

2 vgl. auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Modernisierung des Datenschutzrechtes jetzt – umfassende Novellierung des Bundesdatenschutzgesetzes nicht aufschieben", Anlagenband „Dokumente zum Datenschutz 1999", Teil A I

3 JB 1998, 1.1

4 vgl. 4.7

5 Entwurf zur Änderung des BDSG und anderer Gesetze v. 6. 7. 1999

einschätzung der beabsichtigten Neuregelungen zum Presseprivileg wurde die Gefahr an die Wand gemalt, die *Pressefreiheit* könne durch die Einrichtung betrieblicher Datenschutzbeauftragter und die Einräumung von Auskunftsrechten für die Betroffenen beeinträchtigt werden[6]. Gleichwohl ist damit zu rechnen, dass die zwingend notwendige Novellierung im laufenden Jahr zu Stande kommt.

Nicht aus dem Auge verloren wurde die Zielsetzung, das Datenschutzrecht bei Wahrung der Europakonformität inhaltlich so neuzustrukturieren, dass außer der gebotenen Normenklarheit und Verständlichkeit auch wegweisende Impulse für die Fortentwicklung der Informationstechnik gegeben werden. Die Arbeiten zur Realisierung dieser „zweiten Welle" sollen so bald wie möglich aufgenommen werden, damit Ergebnisse noch in dieser Legislaturperiode vorliegen. Damit verbunden werden könnten Überlegungen, ob nicht die Vorbereitung eines Informationsfreiheitsgesetzes des Bundes, das Gegenstand der Koalitionsvereinbarungen ist, mit diesen Arbeiten koordiniert werden kann.

Auch eine zweite europäische Hausaufgabe blieb unerledigt: Die geplante Angleichung der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) an die *Europäische Telekommunikations-Datenschutzrichtlinie*[7] wurde ebenfalls nicht zu Ende geführt. Die bisher vorliegenden Entwürfe, die deutliche Minderungen der Rechte der Telekommunikationsteilnehmer vorsehen, stoßen auf Kritik der Datenschutzbeauftragten[8].

Europäische Vorgaben werden künftig mehr und mehr die Ausgestaltung und Umsetzung des Datenschutzes bestimmen. So werden weitere bereits verabschiedete (Fernabsatzrichtlinie[9], Richtlinie über die elektronische Signatur[10]) und zu erwartende Richtlinien (insbesondere die Finanzdienstleistungsrichtlinie[11] und die E-Commerce Richtlinie[12]) Auswirkungen auf das deutsche Datenschutzrecht haben.

Die der Europäischen Kommission im Zusammenwirken mit der Gruppe der Datenschutzbeauftragten nach Art. 29 bzw. dem Ausschuss der Regierungsvertreter nach Art. 31 der EU-Richtlinie eingeräumten Befugnisse zur Anerkennung *internationaler Verpflichtungen* (Art. 25

---

6 vgl. hierzu unsere Presseerklärung v. 3.12 1999

7 Richtlinie 97/66/EG des Europäischen Parlaments und des Rates v. 15. 12. 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatssphäre im Bereich der Telekommunikation, ABlEG L 24/1

8 vgl. 5.1

9 Richtlinie 97/7/EG des Europäischen Parlaments und des Rates v. 20. 5. 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABlEG L 144/19

10 Richtlinie 99/93/EG des Europäischen Parlaments und des Rates v. 13. 12. 1999 über gemeinsame Rahmenbedingungen für elektronische Signaturen, ABlEG L 013/12-20

11 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates v. 19. 11. 1998 über den Fernabsatz von Finanzdienstleistungen an Verbraucher, ABlEG C 385/10

12 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (98) 586 endg. Ratsdok. 5123/99

Abs. 6 EU-Richtlinie) sowie zu *Verhaltensregeln* einzelner Gesellschaftsbereiche (Art. 27 EU-Richtlinie) werden zu einer Reihe untergesetzlicher Regelungen führen, die auch die innerstaatlichen Rechtsverhältnisse (etwa durch eine entsprechende Interpretation des Bundesdatenschutzgesetzes) bestimmen werden. So sind im vergangenen Jahr Vorlagen u. a. von der Europäischen Föderation der Direktmarketing-Unternehmen (FEDMA) für die Verwendung von personenbezogenen Daten im Direktmarketing sowie der Internationalen Lufttransport Gesellschaft (IATA) zur Verarbeitung personenbezogener Daten beim internationalen Lufttransport von Passagieren und Fracht vorgelegt worden. Schließlich schicken sich die europäischen Gremien an – ebenfalls verspätet –, die Vorgaben des Amsterdamer Vertrages (Art. 286) umzusetzen und auch für die eigenen Einrichtungen mit einer Verordnung[13] den Datenschutz sicherzustellen.

Gegen Jahresende hat der Ausschuss zur Schaffung einer *Europäischen Grundrechte-Charta* unter dem Vorsitz des ehemaligen Bundespräsidenten Roman Herzog seine Arbeit aufgenommen. Nach einigen gescheiterten Versuchen ist dies ein erneuter Anlauf, das europäische Primärrecht mit Grundrechtsbestimmungen zu krönen. Er geht auf einen Beschluss des Europäischen Gipfels vom Juni 1999 in Köln zurück. Bis Dezember 2000 sollen die Arbeiten abgeschlossen sein und das Dokument vom Europäischen Rat und vom Europaparlament feierlich proklamiert werden. Die Konferenz der Datenschutzbeauftragten hat diese Initiative begrüßt und die Bundesregierung aufgefordert, sich für die Aufnahme eines Grundrechtes auf Datenschutz einzusetzen[14]. Die Bundesministerin für Justiz hat sich inzwischen hierfür ebenfalls eingesetzt, wenn sie auch die Erfolgschancen für Einfügung derartiger „Grundrechte der dritten Generation“ (nach Freiheits- und Sozialrechten) skeptisch beurteilt[15].

Trotz des Beginns einer neuen Legislaturperiode ist im vergangenen Jahr eine Reihe wichtiger *Gesetzgebungsvorhaben* zu Ende geführt worden, die erhebliche datenschutzrechtliche Konsequenzen haben. Vorgesehen war im Rahmen der *Gesundheitsreform 2000* eine enorme Vermehrung des Datenaustausches zwischen den Ärzten und den Krankenkassen. Zwar konnte im Laufe der Diskussion durch die Einführung von Pseudonymisierungsverfahren eine Verbesserung des Entwurfs erreicht werden. In der politischen Auseinandersetzung sind jedoch sowohl die Regelungen zum Datenaustausch als auch diejenigen zur Pseudonymisierung gestrichen worden[16]. Die umstrittene Gesetzgebung zur Bekämpfung der *Scheinselbständigkeit* führte dazu, dass Stellen, die

---

13 Vorschlag einer Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, KOM (99) 337 endg., Ratsdok. 11144/99

14 Entschließung zu „Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union“, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A III

15 Frankfurter Allgemeine Zeitung v. 10. 1. 2000, S. 11

16 vgl. 4.4.2

Werk- oder Honorarverträge vergeben, nunmehr eine Vielzahl personenbezogener Daten erheben und an die Krankenkassen weiterleiten müssen. Beide Gesetzgebungsvorhaben zeigen exemplarisch, dass das Prinzip der Datensparsamkeit, jedenfalls im Bereich der Sozialgesetzgebung, nicht nur nicht beachtet, sondern durch die Schaffung von mehr und mehr Datenströmen konterkariert wird.

Auch im Bereich der Justiz sind Gesetze geschaffen worden, die neue Befugnisse zur Verarbeitung von Daten schaffen: Durch das *DNA-Identitätsfeststellungsgesetz* wird die Befugnis zur Verarbeitung von DNA-Analysen bei Altfällen sowie nach Abschluss von Ermittlungsverfahren erweitert; zur Erleichterung des Täter-Opfer-Ausgleichs können nunmehr auch ohne ausdrückliche Einwilligung Täter- und Opferdaten von der Staatsanwaltschaft an (private) Schlichtungsstellen weitergegeben werden. Auch die Arbeiten an der jahrelang überfälligen Einfügung von Datenschutzvorschriften in die *Strafprozessordnung* sind nicht viel weiter vorangekommen, obwohl die neue Bundesregierung den Entwurf von 1996 erneut eingebracht hat. Auch hier ist ein Zurückdrängen der Datenschutzvorschriften zu Gunsten der Ausweitung von Datenverarbeitungsmöglichkeiten zu beobachten[17].

Signale zur Verbesserung des Datenschutzes sind in einem Eckpunktepapier der Bundesregierung vom Juni 1999 enthalten, in dem die Kryptografie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ hervorgehoben wird. Von Gesetzen, die den Gebrauch kryptografischer Methoden einschränken, soll vorläufig abgesehen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Initiative begrüßt[18].

Gegenüber dieser eher ernüchternden Gesetzgebungsbilanz hat das *Bundesverfassungsgericht* in drei Entscheidungen wegweisende Grundsätze für die Fortentwicklung des Datenschutzes entwickelt.

In seinem lange erwarteten Urteil zur Verfassungsmäßigkeit von *Telekommunikationsüberwachungsmaßnahmen* des *Bundesnachrichtendienstes* hat das Gericht zwar im Wesentlichen die Befugnisse des BND aufgrund des Verbrechensbekämpfungsgesetzes 1994 bestätigt, dabei aber die Bedeutung des Fernmeldegeheimnisses für das Grundrecht auf freie Telekommunikation in einer bisher nicht da gewesenen Weise bestätigt sowie eine ganze Reihe von verfahrensmäßigen Anforderungen an die Durchführung der Telefonüberwachung formuliert. Insbesondere wurde festgelegt, dass sich der Schutz auch auf den der eigentlichen Überwachungsmaßnahme anschließenden Informations- und Datenverarbeitungsprozess sowie die Verwendung der Kenntnisse erstreckt[19].

---

17 vgl. 4.3.1

18 Entschließung zu „Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A III

19 Urteil v. 14. 7. 1999, Az.: 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95; vgl. 4.1.1, 4.1.2, 4.3.1

Eine grundsätzliche Frage, die auch schon in der US-amerikanischen Diskussion über die Fortentwicklung des dortigen Informationsfreiheitsgesetzes eine große Rolle spielte, betrifft die gerichtliche Überprüfung einer Verwaltungsentscheidung, dass Unterlagen geheim zu halten und deshalb an Antragsteller nicht herauszugeben sind. Bei der gerichtlichen Überprüfung müssten zur Wahrung des rechtlichen Gehörs die Unterlagen allen Verfahrensbeteiligten zur Verfügung gestellt werden. Daher wird von der Verwaltung seit jeher geltend gemacht, ihre Beurteilung der *Geheimhaltungsbedürftigkeit* unterliege keiner gerichtlichen Kontrolle. Das in den USA als Ergebnis der Diskussion eingeführte „In-camera-Verfahren" (die Richter entscheiden ohne Verfahrensbeteiligte über die Geheimhaltungsbedürftigkeit) wurde hier für verfassungswidrig gehalten. Das Bundesverfassungsgericht widerlegte dies mit dem Hinweis darauf, dass es zur Effektivität des Rechtsschutzes gehöre, dass das Gericht das Rechtsschutzbegehren umfassend prüfen kann und genügend Entscheidungsbefugnisse besitzt, um drohende Rechtsverletzungen abzuwenden. Dies schließe grundsätzlich eine Bindung des Gerichts an die im Verwaltungsverfahren getroffenen Feststellungen aus. Das Recht der Verwaltung, dem Gericht Akten vorzuenthalten (§ 99 Abs. 1 Satz 2 VwGO) ist mit den Rechtsweggarantieen unvereinbar, soweit die Aktenvorlage auch in den Fällen ausgeschlossen ist, in denen die Gewährung des Rechtsschutzes von der Kenntnis der Verwaltungsvorgänge abhängt. Eine Beschränkung des Akteneinsichtsrechts der Verfahrensbeteiligten kann hingenommen werden, wenn erst durch diese Beschränkung ein effektiver Rechtsschutz möglich ist[20]. Der Berliner Datenschutzbeauftragte hatte schon 1982 die Einführung eines In-camera-Verfahrens in die deutsche Rechtsordnung gefordert[21].

Das Verhältnis zwischen der *Pressefreiheit* und dem Persönlichkeitsrecht von *Prominenten* war Gegenstand eines Urteils, in dem das Gericht betont, dass sich die geschützte Privatsphäre nicht auf den häuslichen Bereich beschränkt, sondern die einzelne Person die Möglichkeit haben muss, sich auch an anderen, erkennbar abgeschiedenen Orten von der Bildberichterstattung unbehelligt zu bewegen. Das Recht kommt auch prominenten Personen zu (in diesem Fall Prinzessin Caroline von Monaco). Es muss allerdings zurücktreten, wenn sich jemand selbst damit einverstanden zeigt, dass bestimmte, gewöhnlich als privat angesehene Angelegenheiten öffentlich gemacht werden: Das allgemeine Persönlichkeitsrecht ist nicht im Interesse einer Kommerzialisierung der eigenen Person gewährleistet. Verstärkten Schutz genießen auch bei Prominenten die Rechte von *Kindern*[22].

---

20 Beschluss v. 27. 10. 1999, Az.: 1 BvR 385/90
21 JB 1982, 6.3
22 Urteil v. 15. 12. 1999, Az.: 1 BvR 653/96

1.2 Datenschutz in Berlin

In seiner letzten Sitzung vor Ende der Legislaturperiode hat das Abgeordnetenhaus das Gesetz zur Förderung der Informationsfreiheit im Land Berlin (Berliner *Informationsfreiheitsgesetz* – IFG -) verabschiedet. Es ist am 30. Oktober 1999 in Kraft getreten. Nach dem Land Brandenburg, das bereits seit 1998 aufgrund eines Verfassungsauftrages über ein derartiges Gesetz verfügt[23], ist das Land Berlin nunmehr das zweite Bundesland, das seinen Bürgerinnen und Bürgern einen Zugang zu den Unterlagen der öffentlichen Verwaltung gewährt, ohne dass diese selbst betroffen sind oder ein besonderes berechtigtes Interesse geltend machen müssen. Die beiden Länder haben damit Anschluss an eine Entwicklung in vielen demokratischen Staaten gefunden, die – allen voran die USA im Jahre 1967 – die Öffnung der Verwaltung als ein Instrument zur demokratischen Meinungs- und Willensbildung geschaffen haben. Wesentliches Anliegen war bei der Gesetzgebung, Informationsfreiheit und Datenschutz in ein angemessenes Verhältnis zu bringen[24].

Datenschutzrechtliche Änderungen des Berliner Landesrechts hat es im Wesentlichen im Bereich der öffentlichen Sicherheit und Ordnung gegeben: Nach der Einführung des *Großen Lauschangriffs* müssen auch in Berlin Berichtspflichten über die Durchführung dieser Maßnahmen eingeführt werden; die Benachrichtigungspflicht, wenn die Speicherung polizeilicher Daten länger als fünf Jahre andauert, wurde gestrichen; das umstrittene Instrument der Schleierfahndung eingeführt. Im Gesetz über den *freiwilligen Polizeidienst* wurden unsere Vorschläge, die Überprüfung der Bewerber normenklar zu regeln, nicht aufgegriffen, das *Katastrophenschutzgesetz* enthält nunmehr eine Rechtsgrundlage für die Weitergabe personenbezogener Daten in Katastrophenfällen. Insgesamt eine Bilanz, die gemischte Gefühle hervorruft[25].

---

23 Akteneinsichts- und Informationszugangsgesetz (AIG) v. 10. 3. 1998, GVBl I, S. 46
24 vgl. 3.1
25 vgl. 4.1.2

2. Technische Rahmenbedingungen

2.1 Die Entwicklung der Informationstechnik

Ohne Zweifel bringt die explosionsartige Ausbreitung des *Internet* die gravierendsten Änderungen der technischen Rahmenbedingungen mit sich: Die kommerziellen Nutzungen des Netzes haben seit Jahren diejenigen im Hochschulbereich überstiegen, von wo der Siegeszug des Internet seinen Ausgang nahm. Aber auch mehr und mehr private Teilnehmer verschaffen sich einen Internetzugang, über den inzwischen jedermann auch WWW-Angebote einstellen kann. Konsequenterweise wird im e-Commerce der wesentlichste Wirtschaftszweig in den nächsten Jahrzehnten gesehen. Die sprunghaften Anstiege der Aktienkurse der Technologie-Unternehmen unterstreichen dies eindrucksvoll.

Zwei Entwicklungslinien zeichnen sich ab, die künftig durchaus zu unterschiedlichen Bewertungen führen können. Zum einen nutzen mehr und mehr Unternehmen die Möglichkeiten des Internet, um Geschäfte abzuwickeln, aber auch um unternehmensintern zu kommunizieren *(Intranet),* wobei diese internen Dienste durchaus auch anderen Unternehmen zur Verfügung gestellt werden können (*Extranet*). Dieser Nutzung des Internet im Rahmen des *B-to-B-Commerce* steht die Nutzung durch den einzelnen Teilnehmer gegenüber, der aus dem Netz nicht nur Informationen abrufen, sondern als Verbraucher (Consumer) die verschiedensten Dienstleistungen in Anspruch nehmen (Banken, Versandhandel, Reisebuchungen usw.) oder sogar selbst aktiv werden kann (z. B. bei elektronischen Versteigerungen). In diesem *B-to-C-Commerce* sieht die Wirtschaft das eigentliche künftige Geschäftsfeld. Auch die öffentliche Verwaltung kann sich diesem Trend nicht verschließen und wird künftig sowohl untereinander als auch mit den Bürgerinnen und Bürgern über das Netz in Verbindung stehen („interaktive Verwaltung“).

Unmittelbar bevor steht zusätzlich die *Mobilisierung* der Technik. Während bisher das Internet fast ausschließlich über feste Anschlüsse genutzt werden konnte, steht mit einer neuen Mobiltelefontechnik *(Wireless Application Protocol* – WAP –) nunmehr die Möglichkeit zur Verfügung, über ein Handy den unmittelbaren Zugang zum Netz herzustellen.

Ermöglicht wurden all diese Entwicklungen dadurch, dass der bereits in den Vorjahren beschriebene Trend zur Entwicklung schnellerer, kleinerer, über größere Speicherkapazitäten verfügender Informationstechnik bei gleichzeitiger Verbesserung des Preis-/Leistungsverhältnisses ungebrochen ist.

Eine Fortsetzung der im Jahresbericht 1998[26] erstmals vorgestellten Tabelle der vor Weihnachten angebotenen Komplettsysteme der gehobenen Leistungsklasse belegt dies eindrucksvoll:

Jahr	Prozessortakt	Arbeitsspeicher	Festplatte	CD-ROM
1997	300 Mhz	32 MB	6 GB	24fach
1998	400 Mhz	64 MB	12 GB	40fach
1999	700 Mhz	128 MB	20 GB	50fach

Diese außerordentlichen quantitativen Fortschritte bewirken, dass auch die Software zunehmend weniger Rücksicht auf Kapazitätseinschränkungen nehmen muss. Optimierungsmaßnahmen zum Umgang mit hardwarebedingten Engpässen verlieren die Rolle, die sie in früheren Zeiten einmal gespielt haben. Sparmaßnahmen beim Speicherplatz, die die Ursache für die befürchteten Probleme beim Übergang ins Jahr 2000 darstellten, verlieren für die moderne Softwareerstellung ebenso an Bedeutung wie die strenge Strukturierung von Datenmodellen und die Zeitoptimierung von Algorithmen. Warum sollen Sachverhalte in syntaktisch streng definierte Datensätze korsettiert werden, wenn Textretrievalsysteme den verbal beschriebenen Sachverhalt genauso schnell und viel genauer erschließen können?

Informationstechnik – nur ein Segen?

Vier Themen aus dem Berichtsjahr geben Anlass zur Sorge um die zukünftige Informationsgesellschaft, denn sie manifestieren die zunehmende *Abhängigkeit* der Gesellschaft von informationstechnischen Systemen. Die Gefahr, dass die Grenzenlosigkeit der kommunikativen Beziehungen undemokratischen Machtstrukturen und Machtinstrumenten Vorschub leistet, ist nicht von der Hand zu weisen. Die Grundrechte geraten in Gefahr – nicht, weil die Technik dies bedingt, sondern ihre Potenziale dazu ausgenutzt werden, Abhängigkeiten zu erzeugen.

Kaum ein Thema hat im vergangenen Jahr die Fachwelt so beschäftigt wie die *Jahr-2000-Problematik* (Year 2 Kilo -Y2K-, Millennium-Bug). Zum Jahresende 1999 war das Thema auch in der Presse Hauptthema. Die offenkundige Anfälligkeit und Angreifbarkeit informationstechnischer Systeme einerseits und die Abhängigkeit der gesellschaftlichen Infrastrukturen von der Verfügbarkeit dieser Strukturen machten die Gefährdungen der IT-Sicherheit zu einem Medienereignis.

In den 60er und 70er Jahren mussten die Programmierer so sehr mit dem Speicherplatz geizen, dass sie bei den *Datumsangaben* für die Jahreszahl nur die letzten beiden Stellen vorsahen. In diesem Format wurden auch die arithmetischen Operationen, die üblicherweise mit Jahreszahlen erfolgen – vor allem Subtraktionen zur Ermittlung eines

[26] JB 1998, 2.1

abgelaufenen Zeitraums -, programmiert. Jedem Programmierer dürfte klar gewesen sein, was dies bei einem Jahrhundertwechsel bedeutet, aber offensichtlich bestand angesichts des auch damals schon dramatisch schnellen Fortschritts der Informationstechnik die Erwartung, dass die Programme die Jahrhundertwende nicht erleben würden. Die Entwicklung moderner Programme baut jedoch auf alten Programmen auf. Manches Programmmodul aus den 70er Jahren ist noch Bestandteil von Programmen der 90er Jahre und so erklärt sich, dass selbst für einige Programmversionen, die vor drei Jahren neu auf den Markt kamen, eine 2000-Garantie nicht gegeben werden mochte.

Eine weitere Gefahr wurde darin gesehen, dass in vielen technischen Systemen technische Bauteile eingesetzt sind, die zeitliche Steuerungen bewirken sollen, aber nicht als 2000-fähig angesehen wurden (sog. *Embedded Chips*). Dies hätte z. B. bei wartungsbedürftigen Systemen dazu führen können, dass diese plötzlich „erkennen", dass sie seit fast 100 Jahren nicht gewartet wurden, und sich daher sicherheitshalber ausschalten müssten.

Der Presse war zu entnehmen, dass für die Herstellung der 2000-Fähigkeit bei informationstechnischen oder informationstechnisch gesteuerten Systemen 500 – 1000 Milliarden Dollar weltweit investiert werden würden. Kritisch war ebenfalls zu vernehmen, dass ausgerechnet die sonst so ordentlichen Deutschen nur mühsam aus ihrer Gelassenheit zu wecken waren. Da waren Kassandrarufe nicht mehr zu vermeiden: Ein sommerliches Expertenforum der Süddeutschen Zeitung beschrieb „die Nacht, in der die Welt aus dem Takt geraten wird", auf die „mindestens 10 % aller Firmen nicht vorbereitet sind"[27]. Wenigstens ein Fragezeichen leistete sich die Computerwoche beim Thema der 29. Woche: „Führt das Jahr-2000-Problem 350 000 Firmen in die Pleite?"

Wir können inzwischen auf die Silvesternacht 1999/2000 zurückblicken und zurückfragen: War was? Jedenfalls fiel das angekündigte Millennium-Desaster aus. Einige Meldungen über Marginalstörungen wurden verbreitet, die in anderen Nächten keine Nachricht wert gewesen wären. Das eine oder andere Systemprotokoll zeichnete seine ordnungsgemäße Funktion mit einer merkwürdigen Codierung der Jahreszahl 2000 auf, manch ein unangepasster Alt-PC war in das Jahr 1980 zurückgefallen und musste mit ein paar Kommandos wieder in das richtige Zeitalter gebracht werden.

Ob der ruhige Verlauf der Millenniumsnacht nun auf die kostspieligen und sorgfältigen Vorbereitungen zurückzuführen ist oder alles nur Panikmache war, die der IT-Industrie mächtige Zusatzgewinne einbrachte, weil der von ihr selbst in die Welt gesetzte Computerfehler

27 Süddeutsche Zeitung v. 17./18. 7. 1999, S. 13

weltweit einen Schub von Systemmodernisierungen und Beratungsaufträgen bewirkte, wird man wohl nie genau sagen können. Einerseits dürfte sicher sein, dass einige wichtige Maßnahmen dem Zusammenbruch wichtiger Infrastrukturen entgegengewirkt haben. Andererseits wurde vor dem Jahreswechsel die unterschiedliche Intensität der Vorbereitungen in den verschiedenen Ländern beklagt, die sich aber offensichtlich nicht in einer Unterschiedlichkeit der Folgen auswirkte. Dies lässt darauf schließen, dass auf bestimmten weniger wichtigen Ebenen Gelassenheit eher angebracht war als hektischer Aktionismus.

Die Jahr-2000-Problematik wird die Entwicklung der Informationstechnik in zweierlei Hinsicht vorantreiben: Zum einen hat sie – hoffentlich nicht nur für den Augenblick – der breiten Öffentlichkeit, aber auch den öffentlichen Stellen und privaten Unternehmen in Berlin deutlich gemacht, dass die Sicherheit der Informationstechnik mehr ist als die Spielwiese von angeblich den Fortschritt hemmenden Datenschützern. Zum anderen haben die Anpassungsarbeiten weltweit einen überdurchschnittlichen Modernisierungsschub bei den informationstechnischen Systemen und Anwendungen erbracht.

Die Verletzlichkeit der Informationsgesellschaft, die uns mit dem beschriebenen Jahr-2000-Problem eindrucksvoll geschildert, zum Glück aber nicht vorgeführt wurde, gilt inzwischen auch als Aspekt einer modernen Kriegsführung. Seit dem Irak-Krieg im Jahre 1991, besonders intensiv aber im Zusammenhang mit dem Kosovo-Konflikt, wird offen darüber diskutiert, ob nicht durch Hacking oder Schadsoftware wie Computerviren, Logische Bomben, Trojanische Pferde oder Trapdoors die Steuerungssysteme von Informationsgesellschaften effizienter ausgeschaltet werden können als durch Bombardements[28]. Auch werden spezielle Sprengwaffen diskutiert, mit denen gezielt empfindliche Informationstechnologie ge- oder zerstört werden kann[29] (*„Information Warfare"*).

Die Spekulationen bewegen sich vor einem realen Hintergrund: Nach wie vor werden erfolgreiche Hackerangriffe und Verbreitungen von Computerviren bekannt. Sie treffen nach wie vor und weltweit verbreitet auf Leichtsinn und Verantwortungsträger, die den Schutz ihrer Informationstechnik für zweitrangig halten. Werden diese Angriffsformen weiter professionalisiert, dann können auch militärisch unterlegene Parteien mit Information Warfare den überlegenen, von Informationskanälen abhängigen Gegner empfindlich treffen. Eine vom Präsidenten der USA eingesetzte Kommission zur „Absicherung kritischer Infrastrukturen" beschäftigt sich seit 1998 mit dieser Problematik, weil gerade in der Verwundbarkeit im „Cyber War" große Risiken für das Land gesehen werden[30].

---

28 DER SPIEGEL 37/1999, S. 288 ff.

29 vgl. z. B. A. Baumann: Bitskrieg – Information Warfare: Krieg im Informationszeitalter, c't 1998, Heft 18, S. 80 ff.

30 Die Welt v. 17. 3. 1998, S. 7

Die unbegrenzten Möglichkeiten zur Informationsverarbeitung erlauben die weltweite heimliche Beobachtung der Kommunikationsvorgänge und ihrer Inhalte sowie die Nutzung der Ergebnisse zum Nachteil der Betroffenen und zur Durchsetzung nationaler oder anderweitig einseitiger politischer und wirtschaftlicher Interessen. Die *globale Telekommunikationsüberwachung* durch die US-amerikanische Sicherheitsbehörde NSA mit ECHELON war Gegenstand unserer Ausführungen an dieser Stelle im Vorjahr[31]. Dass die Sicherheitsinteressen von Staaten und die Aufrechterhaltung von Sicherheit und Ordnung in einem Staat der informationellen Selbstbestimmung Grenzen auferlegen, ist anerkannt. Dass für diese Ziele auch die neuesten Entwicklungen in der Informationstechnik eingesetzt werden, ist selbstverständlich. Welche Grenzen dort zu setzen sind, nimmt in den Tätigkeitsberichten der Datenschutzbeauftragten auf der Welt einen namhaften Raum ein. Die „Kinder von Orwells Großem Bruder" sollten ursprünglich den nationalen Sicherheitsinteressen dienen. Am Beispiel von ECHELON wird allerdings deutlich, dass dann, wenn die politische Entwicklung bestimmte Sicherheitsinteressen überflüssig gemacht hat, die Überwachungssysteme auf neue Ziele ausgerichtet werden, z. B. auf nationale wirtschaftliche Interessen.

In der Privatwirtschaft bemühen sich die Unternehmen um ihre Kunden, um ihre Konkurrenzfähigkeit sowohl im Inland als auch im Ausland zu sichern. *Kundenbindung* wird immer wichtiger, und diese ist umso besser, je genauer man den Kunden kennt. Um die Daten der Kunden zu erhalten, ist kaum ein Aufwand mehr unwirtschaftlich. Kunden- und VIP-Karten, verbunden mit Einkaufsvergünstigungen, verlocken dazu, persönliche Details zu offenbaren, die der *Direktmarketing- und Direktwerbung* die informationelle Basis liefern. Es ist sicher praktisch, die Kunden bei Bargeschäften namentlich zu kennen, aber nötig ist es nicht. Wenn man genügend Details über die Verhaltens- und Konsummuster der unterschiedlichen Kundenkategorien kennt, kann die Betreuung, Beratung und Umwerbung ebenfalls recht zielgenau erfolgen.

Im Jahresbericht 1997[32] haben wir über das *Data Mining* in *Data Warehouses* berichtet, also über die modernen Datenverwaltungs- und -recherchesysteme, die auf der Grundlage relationaler Datenbankkonzepte und unter Ausnutzung des technischen Fortschritts heterogene Datenbestände nach allem durchforschen, was der Steuerung von Unternehmen dient, hauptsächlich Angaben über Kunden, Kundengruppen und Geschäftspartner.

---

31 JB 1998, 2.1, vgl. 5.1
32 JB 1997, 2.1

In diesem Jahr erfinden wir unser Szenario nicht selbst. Wir zitieren einen Anbieter fortgeschrittener Warehouse- und Datenanalysesysteme[33]:

> *„Ein Hersteller für Freizeitbekleidung verkauft Paul Müller ein Paar Wanderstiefel über seine Web-Site. Ein anwenderfreundlicher Bedienerhinweis bietet Herrn Müller zielgruppengleiche Produkte wie Windjacken, Wandersocken, Hüte und Wanderartikel an. Er lehnt ab und besucht einen Bereich der Web-Site, der vom Long Trail in New England handelt. Später erhält er eine E-Mail über Bergstrecken in Vermont, die eine direkte Verknüpfung zu anderen Internet-Seiten des Herstellers enthält, auf denen leichtgewichtige Zelte für Bergsteiger angeboten werden. Paul Müller wählt ein Zelt aus und bestellt anschließend noch einige Kochutensilien. Ein Jahr nach seinem Kauf erhält er einen personalisierten Mobiltelefonanruf und wird gefragt, wie er mit seinen Wanderstiefeln zufrieden war, und bekommt neue Wanderstiefel angeboten, die er sofort am Telefon bestellt."*

Man sieht, in welche Lebensbereiche derartige Systeme eindringen – zunächst ohne Rücksicht auf den Willen der Betroffenen.

Alle Beispiele belegen die Gefahr, dass die Rahmenbedingungen der Informationstechnik die Tendenz fördern, den Menschen zum Objekt fremder Einflussnahme zu machen. Für den Datenschutz ergeben sich hier ganz neue Aufgabenstellungen.

Global Unique Identifiers (GUID) – Futter für die Nachkommen des Großen Bruders?

Zu Beginn des Jahres 1999 freute sich die Computerwelt über die Markteinführung von Intels neuester Chipgeneration, dem *Pentium-III-Prozessor,* über weiter verbesserte Taktraten und zusätzliche Funktionen. Die Firma war aber sehr erstaunt, als sich in den Jubel erhebliche Verärgerung über ein Leistungsmerkmal mischte, das die Sicherheit der Benutzer – z. B. beim Online-Banking – verbessern sollte: Die *Chip-Identifikationsnummer* (Chip-ID), die bei der Internet-Kommunikation mitgesendet oder von außen abgefragt werden kann. Mit der Chip-ID könne man den Rechner sicher identifizieren und man habe so ein zusätzliches Merkmal, um die Authentizität eines Benutzers bei seinen Bankgeschäften oder anderen Aktivitäten im elektronischen Handel besser gewährleisten zu können.

Es gab massive Kritik in den USA, die mit der Einführung des Pentium-III auch nach Europa überschwappte. Der Widerstand formierte sich aus der Furcht, mit der Identifizierung der eigenen Rechner im Internet könnten die Aktivitäten und Kommunikationsgewohnheiten

---

[33] E-Business – Kundenbeziehungen verbessern – Ein Whitepaper, erstellt von MicroStrategy (Incorporated), 1999, S. 6

der Websurfer unbemerkt beobachtet und aufgezeichnet werden. Intel stellte sich der öffentlichen Diskussion, auch mit den deutschen Datenschutzbeauftragten. Das Unternehmen kündigte eine Software an, die es dem Benutzer ermöglichen sollte, die Aussendung der Chip-ID im Einzelfall zu unterbinden. Intel forderte die PC-Hersteller auf, die Chip-ID im BIOS (Basic Input Output System) der PCs standardmäßig zu deaktivieren, und kündigte an, die Zusammenarbeit mit allen Software-Herstellern bei Applikationen unter Verwendung der Chip-ID zu beenden sowie die Fertigstellung und Weiterentwicklung solcher Software zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder nahmen sich des Themas an[34]. Dabei monierten sie, dass die Entwicklung der Informationstechnik zu Industriestandards und Produkten führt, die selbst von Fachleuten kaum noch sicher durchschaut werden können. Die Firma Intel bedauerte, dass gerade ihr Produkt zum Gegenstand einer solchen Entschließung gemacht wurde. Tatsächlich kommt dem Marktführer das Verdienst zu, das Thema in der Öffentlichkeit vertreten zu haben.

Gegenstand der Entschließung war auch eine Meldung, die wenig später weltweit für Aufregung sorgte. Amerikanische Fachleute hatten entdeckt, dass der Software-Marktführer *Microsoft* bei der Online-Registrierung des Betriebssystems WINDOWS 98 jedem Kunden eine weltweit eindeutige Nummer *(HWID – Hardware Identifikationsnummer)* zuordnet und auf dem Kundenrechner abspeichert. Die Nummer kann aus dem Rechner abgefragt werden.

Auch dieses Hilfsmittel sollte nur einem guten Zweck dienen: Mit der Identifizierung der Software könne man dem Nutzer besser bei der Lösung von Problemen helfen, keinesfalls wolle man jedoch das Nutzerverhalten zu Marketingzwecken verfolgen. Vor allem aber würden die Daten nur dann übertragen, wenn der Benutzer bei der Online-Registrierung ausdrücklich wünscht, dass seine Systemdaten übertragen werden. Dass dies dann nicht stimmte und damit auch gegen den Willen der Nutzer die Daten übertragen wurden, führte Microsoft auf einen Programmierfehler zurück, der mit dem nächsten Service-Pack beseitigt werden solle. Außerdem wolle man alle Daten in den eigenen Datenbanken löschen, deren Übermittlung gegen den Willen der Kunden geschah.

Nachdem entdeckt wurde, dass eine eindeutige Nummer auch mit Dokumenten versandt wird, die mit Hilfe des Microsoft-Produkts *Office 97* erzeugt werden, erläuterte Microsoft der zuständigen Datenschutz-Aufsichtsbehörde in Deutschland, dass es sich dabei um eine Nummer handele, die mit der HWID nichts zu tun hätte, sondern eine

---

[34] Entschließung zu „Transparente Hard- und Software“, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A I

GUID, die ein Dokument dem Rechner zuordnen kann, in dem es entstanden ist. Diese Nummer diene der Zuordnung von Dokumenten, die in einem Netz zirkulieren, und soll damit die Zusammenarbeit der Netzteilnehmer erleichtern.

Microsoft wies darauf hin, dass die GUID im Unternehmen nicht gespeichert würde, und kündigte an, Programmberichtigungen auf ihrer Website zugänglich zu machen, die verhindern würden, dass neuen Dokumenten die GUID angehängt wird, ferner ein Löschprogramm für die GUIDs bestehender Dokumente dort anzubieten und last but not least in Office 2000 auf die GUID ganz zu verzichten. Obwohl die Gerüchte in der Fachpresse nicht ganz verstummten, Microsoft habe diese Versprechungen nur zur Beruhigung der deutschen Datenschutz-Aufsichtsbehörden abgegeben, ist von der Ernsthaftigkeit der Absichten des Marktführers auszugehen.

In der Folge gab es immer wieder Meldungen über heimliche Hard- und Softwaremerkmale, die auf die informationelle Selbstbestimmung der Benutzer abzielen:

- Ein kleines und offenbar gern benutztes Spaßprogramm der Softwarefirma Comet Systems übertrug heimlich GUIDs der Nutzer an die Firma, angeblich nur für die Abrechnung mit den eigenen Kunden[35].
- Ein Programm zur Musikwiedergabe soll über längere Zeit heimlich Identitätsnummern an den Software-Hersteller RealNetworks übermittelt haben[36].
- Der Schlüssel „NSAKEY“ in den WINDOWS-Betriebssystemen von Microsoft wirft die Frage auf, ob das ein Generalschlüssel für den amerikanischen Geheimdienst NSA zum Lesen verschlüsselter Nachrichten ist oder – wie Microsoft behauptet – ein Mittel, das es dem NSA ermöglicht, die Einhaltung amerikanischer Exportbedingungen für Verschlüsselungssoftware zu überwachen?[37].

All diese Meldungen und Mutmaßungen haben einen realen Hintergrund: Hersteller bauen heimlich unbekannte Funktionen und Leistungsmerkmale in Hard- und Software ein, die sich in bestimmten Zusammenhängen gegen die Interessen der Benutzer richten – auch wenn das Gegenteil beteuert wird. Daten über Kunden und deren Verhalten sind in der künftigen Informationsgesellschaft Dinge, für die hohe Preise bezahlt werden, wenn dem nicht durch hinreichende Maßnahmen begegnet wird.

---

35 Berliner Morgenpost v. 17. 12. 1999, S. 15
36 PC-Magazin, Januar 2000, S. 23
37 Handelsblatt v. 8. 9. 1999, S. 55

2.2 Datenverarbeitung in Berlin

Natürlich bleibt Berlin von den globalen Entwicklungen in der Informationstechnik und ihren Anwendungen nicht unberührt. Dies zeigen vielfältige Aktivitäten in der Stadt: Viele private Unternehmen beschäftigen sich mit der Herstellung von Soft- und Hardware, entwickeln Anwendungen der Informations- und Kommunikationstechnik und bieten Dienstleistungen der Datenverarbeitung an. Ein Blick auf die Unternehmen, die an der Berliner Börse gehandelt werden, zeigt, dass es auch in Berlin Unternehmer gibt, die neue Ideen für das weltweite Datennetz wirtschaftlich erfolgreich umsetzen können. Im Register der in Berlin tätigen und nach § 32 Bundesdatenschutzgesetz meldepflichtigen Dienstleistungsunternehmen in der Datenverarbeitung finden sich auch die wichtigsten Marktführer wieder.

Erhebliche Anstrengungen unternimmt der Senat, allen voran die Senatsverwaltung für Wirtschaft und Betriebe, die Entwicklung der Informationstechnik in Berlin zu fördern. So bündelt die Landesinitiative *„Projekt Zukunft – Der Berliner Weg in die Informationsgesellschaft“* eine Reihe öffentlicher und privater Projekte. Unser Vorschlag, in diesen Projekten die Bedeutung des Datenschutzes als Qualitätsmerkmal deutlich zu machen, hat auch im Berichtsjahr kaum Resonanz gefunden.

Auch in der Berliner Verwaltung, über deren Aktivitäten wir aufgrund der gesetzlichen Aufgabenzuweisung und bestehenden datenschutzrechtlichen Transparenzgeboten einen genaueren Überblick haben, ist die technische Entwicklung trotz der finanziellen Engpässe im Berliner Staatshaushalt nicht stehen geblieben. Es ist längst erkannt, dass ohne intensiven Einsatz der Informationstechnik eine moderne Verwaltung nicht ökonomisch funktionieren kann. Es ist ferner erkannt, dass sich auch die öffentliche Verwaltung der weltweiten Dynamik und Faszination des Internet nicht entziehen kann.

Stadtinformationssystem Berlin.de

Mit dem *Stadtinformationssystem Berlin.de* befindet sich eine umfangreiche Webpräsentation des Landes im kontinuierlichen Aufbau. Wichtige Informationen für Berlins Bürger und potenzielle Besucher werden zur Verfügung gestellt und ersparen ihnen die häufig zeitraubenden Erkundigungen. Interaktive Bürgerdienste, die über die reine Bestellung von Informationsmaterial und dem Downloaden von Formularen hinausgehen, werden allerdings noch nicht angeboten. Für verbindliche und formelle interaktive Kontakte zwischen Bürger und Verwaltung fehlt es noch an den technischen Voraussetzungen zur Gewährleistung der Authentizität und Verbindlichkeit auf dem Netz.

2.2

Wir haben im letzten Jahresbericht ausführlich zu den datenschutzrechtlichen und IT-sicherheitstechnischen Fragestellungen dieses Projektes Stellung genommen[38]. Das Projekt Berlin.de hat in der Zwischenzeit auch Kritik erfahren müssen, die nichts mit dem Datenschutz zu tun hat. Kritisiert wurden die umständlichen Suchmöglichkeiten, die es dem Bürger schwerer als nötig machten, das im Angebot zu finden, was er sucht. Es fehlt eine Suchmaschine und vor allem ein Verwaltungsführer, der die verschiedenen Angebote verknüpft. Daraufhin kündigte der Senat eine bessere Koordination und die baldige Realisierung von interaktiven Verwaltungsdiensten und der elektronischen Unterschrift an.

Die datenschutzrechtliche Relevanz der *interaktiven Bürgerdienste* im Rahmen von Berlin.de veranlasste uns zu einer Umfrage in den Haupt- und Bezirksverwaltungen nach dem jeweiligen Realisierungsstand solcher Dienste. Das Ergebnis machte deutlich, dass die Bezirke in Berlin.de keine interaktiven Dienste anbieten. Einige Bezirke haben eigene Angebote aufgebaut, teilweise mit einfachen interaktiven Elementen wie z. B. E-Mail. In der Hauptverwaltung besteht offenkundig mehr Akzeptanz zu Berlin.de, jedoch werden interaktive Dienste ebenfalls kaum angeboten. Im Geschäftsbereich der Senatsverwaltung für Wissenschaft, Forschung und Kultur werden interaktive Dienste im Bereich der Hochschulen und einigen kulturellen Einrichtungen bereits angeboten, jedoch nicht im Rahmen der zentralen Darstellung Berlins im Internet.

Vereinheitlichung und Zusammenführung der Datenstrukturen (VeZuDa)

Mit dem *VeZuDa-Projekt* soll eine Infrastruktur im *Berliner Landesnetz* geschaffen werden, die die einheitliche und verfahrensübergreifende Verwendung von *Grunddaten zu Personen bzw. Grundstücken* zum Ziele hat. Einmal von einer besonders dafür ausersehenen Behörde erfasst, sollen diese Grunddaten allen anderen Verfahren als aufrufbare Objekte zur Verfügung gestellt werden, sobald sie erhoben werden sollen. Kommt ein Bürger also in eine Behörde, so genügt seine sichere Identifizierung, etwa durch Vorlage des Personalausweises, und schon können die im Melderegister verfügbaren Grunddaten in Form einer „Datenkapsel“ über das Netz zur Verfügung gestellt werden. Aufwendige und fehleranfällige Zweiterfassungen können unterbleiben. Dies führt zu Datenbeständen, die zueinander konsistent und mit größerer Wahrscheinlichkeit als zuvor auch richtig sind. Dies ist aus datenschutzrechtlicher Sicht zu begrüßen. Folgende datenschutzrechtliche Problemfelder sind jedoch zu beachten:

---

38 JB 1998, 2.2

Nach § 10 Abs. 1 BlnDSG sind die Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben. Bei Nutzung von VeZuDa-Datenkapseln werden die Daten beim Quellverfahren abgerufen, also nicht beim Betroffenen erhoben. Dies ist nur dann zulässig, wenn der Aufruf der entsprechenden Datenobjekte mit *Kenntnis der Betroffenen* erfolgt und mit diesen auf Richtigkeit geprüft werden kann.

Bei dem VeZuDa-gestützten Zugriff handelt es sich um ein *automatisiertes Abrufverfahren,* für das nach § 15 BlnDSG eine gesetzliche Ermächtigung und eine Verordnung für nähere Festlegungen existieren muss. Für den Zugriff auf *Eigentümerdaten* im *Automatisierten Liegenschaftsbuch* liegt mit der Liegenschaftskataster-Abrufverordnung (LiKa-AbrufVO) eine solche Rechtsverordnung vor.

Es ist datenschutzrechtlich geboten, dass sich der *Umfang der Grunddaten* auf das Erforderliche beschränkt. Entweder werden also die Datenkapseln auf die einzelnen Erfordernisse des abrufenden Verfahrens angepasst oder aber es wird eine einheitliche Datenkapsel definiert, die jedoch nur die Durchschnittsmenge der erforderlichen Daten enthalten darf, weil anderenfalls viele Verwaltungsverfahren mehr Daten erhalten, als sie benötigen.

Die Zugriffsbeschränkung auf das jeweils Erforderliche ist durch *technische Maßnahmen* sicherzustellen. Der Zugriff auf solche Datenkapseln darf nur erfolgen können, wenn ein konkreter Bearbeitungsfall vorliegt. Wenn dieses nicht durch andere technische Maßnahmen abgesichert werden kann, muss eine Protokollierung erfolgen, die auch den Abfragegrund, z. B. durch Aufzeichnung des Aktenzeichens im Anwendungsverfahren, aufzeichnet.

Eine *Verschlüsselung* der personenbezogenen Daten bei der Übertragung im Berliner Landesnetz ist erforderlich.

Eine weitere Frage war die Nutzung personenbezogener *Echtdaten* bei der Erprobung der VeZuDa-Funktionalitäten. Dazu haben wir empfohlen, die für den Testbetrieb erforderlichen Testdaten von zwei Verfahren durch eine Einwegverschlüsselung nach dem Vorbild von UNIX-Passwörtern zu verschlüsseln. Dies führt dazu, dass nicht rekonstruierbare Pseudonyme entstehen, die jedoch für gleiche Ausgangsnamen gleich sind, so dass der gegenseitige Zugriff realistisch nachvollzogen werden kann.

Weitere Verfahren

Nähere Ausführungen zu den Fachverfahren, bei denen wir beteiligt wurden, finden sich an anderen Stellen dieses Berichts:

- Integrierte Personalverwaltung (IPV)[39]

[39] vgl. 4.4.1

- Sozialhilfeverfahren BASIS I und BASIS II[40]
- Datenerhebung Jugend+Sucht[41]
- Querschnittscontrolling beim Programm „Integration durch Arbeit" – IdA[42]
- Elektronisches Ticketing bei der BVG[43].

Unsere Aufmerksamkeit fanden weiterhin u. a. die Verfahren Neues Einwohnerwesen (EWW-neu), Neues Berliner Rechnungswesen (NBR), Handelsregister (HAREG), Elektronisches Grundbuch (SOLUM STAR), Verbund der Öffentlichen Bibliotheken Berlins (VÖBB), IT-Verfahren der Hochschulbibliotheken (ALEPH 500), IT-Verfahren Justizvollzugsanstalten (BASIS 2000).

Informationstechnische Sicherheit in Berlin

Anfang Januar 1999 ist die *IT-Sicherheitsrichtlinie* des Landes veröffentlicht worden und damit offiziell in Kraft getreten, nachdem auf Beschluss des IT-Koordinations- und Beratungsausschusses (IT-KAB) die Anwendung der Richtlinie bereits vorher vereinbart worden war. Über die Regelungen der IT-Sicherheitsrichtlinie haben wir bereits im Jahresbericht 1998 ausführlich berichtet[44].

Die IT-Sicherheitsrichtlinie stellt der Verwaltung zur Aufgabe, methodische Überlegungen zur Gewährleistung der informationstechnischen Sicherheit und – damit stets untrennbar verbunden – zur Umsetzung der technisch-organisatorischen Maßnahmen zum Datenschutz nach § 5 Abs. 3 BlnDSG anzustellen. Eine solche Herangehensweise ist offenkundig neu für viele Bereiche der Verwaltung, denn die nach der IT-Sicherheitsrichtlinie geforderten IT-Sicherheitskonzepte auf der Grundlage anerkannter Methoden, die auf einer Risikoanalyse aufbauen, sind noch sehr rar.

Die IT-Sicherheitsrichtlinie beschreibt nicht nur die Grundsätze der Sicherheitspolitik für die im Lande in den Einsatz kommenden informations- und kommunikationstechnischen Systeme, Infrastrukturen und Anwendungen und weist auch nicht nur die Verantwortung auf bestimmte Funktionsträger zu, sondern macht auch Vorgaben zum methodischen Vorgehen und zur Umsetzung.

Logisch, organisatorisch und räumlich zusammengehörende Bereiche, die einheitlichen Sicherheitsanforderungen zu genügen haben, sind als *Sicherheitsdomäne* auszuweisen. Für diese Sicherheitsdomänen sind *Sicherheitskonzepte* zu erarbeiten und umzusetzen. Es hängt vom Schutzbedarf ab, ob es ausreicht, das IT-Grundschutzhandbuch des

40 vgl. 4.4.3
41 vgl. 4.4.3
42 vgl. 4.4.3
43 vgl. 4.6.3
44 JB 1998, 2.2

Bundesamtes für Sicherheit in der Informationstechnik (BSI) anzuwenden, oder ob ganz oder teilweise das komplexere Verfahren nach dem IT-Sicherheitshandbuch des BSI anzuwenden ist.

Die Sicherheitskonzepte müssen den Anwendungsbereich exakt beschreiben und eine Risikoanalyse enthalten, die die konkreten Rahmenbedingungen der Sicherheitsdomänen im Einzelfall beschreibt und die daraus folgenden Risiken für die informationstechnische Sicherheit benennt. Die Maßnahmen zur Verringerung der Risiken auf ein tragbares Maß sind zu beschreiben und es ist im Rahmen einer Restrisikoanalyse zu bewerten, ob damit alle untragbaren Risiken auf ein tragbares Maß verringert worden sind. Es müssen ferner die Verantwortlichen für die Umsetzung benannt und ein Umsetzungsplan erstellt werden, der Prioritäten benennt sowie Fristen und Kosten.

Explizit benannt werden die Sicherheitskonzepte für die zentrale IT-Infrastruktur (z. B. *Berliner Landesnetz, Sicherheitsrechenzentrum)*, die vom Landesbetrieb für Informationstechnik verantwortlich betreut wird, die behördenbezogenen Sicherheitskonzepte, die für jede Behörde, ggf. aber auch für abgrenzbare Behördenteile, anzufertigen sind, sowie die verfahrensspezifischen Sicherheitskonzepte, die sich auf die besonderen Bedingungen eines IT-Verfahrens beziehen.

Wenn wir über neue IT-Verfahren *unterrichtet* werden, beschränken sich häufig die Angaben zu den technisch-organisatorischen Maßnahmen auf die Zitierung einschlägiger, aber natürlich allgemein und pauschal gehaltener gesetzlicher Vorschriften oder – wenn es hochkommt – auf die Kurzbeschreibung der durch die Betriebs- und Standardsoftware bzw. Standardrechner bereitgehaltenen Werkzeuge mit Sicherheitsrelevanz. Sicherheitskonzepte, die den oben beschriebenen Anforderungen nahe kommen, sind selten und müssen in unseren ersten Stellungnahmen zu den Verfahren grundsätzlich angemahnt werden. Rückfragen, die wir auf solche Forderungen erhalten, machen deutlich, dass die notwendigen methodischen und inhaltlichen Kenntnisse für die Erstellung von Sicherheitskonzepten dünn gesät sind. Deshalb ist es erstaunlich, dass entsprechende Schulungsangebote der Verwaltungsakademie so zurückhaltend angenommen werden, dass Kurse mangels ausreichender Meldungen vom Programm genommen zu werden drohen.

Mit unserer Broschüre „Datenschutz und informationstechnische Sicherheit beim *PC-Einsatz",* die auf dem IT-Grundschutzhandbuch des BSI beruht, liegt den IT-Fachleuten der Berliner Verwaltung eine weitere Unterlage zur Erstellung von Sicherheitskonzepten zur Verfügung, die in mindestens 95 % aller IT-Anwendungen des Landes einschlägig sein dürfte.

In der IT-Sicherheitsrichtlinie ist auch festgelegt worden, dass unter der Leitung der Senatsverwaltung für Inneres eine ständige Arbeitsgruppe IT-Sicherheit des IT-KAB unter Beteiligung des Rechnungshofs

von Berlin und des Berliner Beauftragten für Datenschutz und Akteneinsicht eingerichtet wird. Diese Arbeitsgruppe berät zu allen Fragen des sicheren Einsatzes von Informationstechnik, die von behördenübergreifender Bedeutung sind. Hauptschwerpunkte sind die Erarbeitung eines jährlichen Sicherheitsberichtes und eines dazugehörigen Umsetzungsplanes. Des Weiteren soll die IT-Sicherheitsrichtlinie und deren operationalisierbare Ausgestaltung ständig fortgeschrieben werden.

Der jährliche *Sicherheitsbericht* soll Aussagen über die Wirksamkeit von Sicherheitsmaßnahmen, eine Analyse neuer Risiken und darauf aufbauende Maßnahmevorschläge beinhalten. Der Sicherheitsbericht ist die Basis für einen durch den IT-KAB zu beschließenden Umsetzungsplan. Dem Umsetzungsplan muss dabei besondere Bedeutung zukommen. Die Erfahrung hat gezeigt, dass die Erarbeitung von Datenschutz- und IT-Sicherheitskonzepten zwar an vielen Stellen bereits durchgeführt wird, eine Umsetzung jedoch nur sehr zögerlich und bruchstückhaft erfolgt. Das Ergebnis des Sicherheitsberichtes hinsichtlich der Umsetzung der IT-Sicherheitsrichtlinie stellt sich sehr unterschiedlich dar: Positive Entwicklungen gibt es bei der Erarbeitung und Umsetzung behördenspezifischer Sicherheitskonzepte und für den Einsatz von gestaffelten Firewalls[45] beim Anschluss an das Berliner Landesnetz. Die hierzu erforderlichen Maßnahmen wurden in vielen Behörden bereits umgesetzt oder sind bis zum Ende des Jahres 1999 geplant. Voraussetzung hierfür ist jedoch, dass auch bei der bekannt kritischen Haushaltslage die benötigten finanziellen Mittel bereitgestellt werden.

Auch die Arbeitsgruppe beklagt die unbefriedigende Situation bezüglich der Sicherheit von IT-Verfahren. So verfügen kleinere bzw. dezentrale IT-Verfahren noch nicht über ein Sicherheitskonzept und bei den IT-Großverfahren bestehen teilweise erhebliche Mängel in der Umsetzung einzelner Regelungen der IT-Sicherheitsrichtlinie bzw. der IT-Sicherheitsstandards. Dringender Handlungsbedarf besteht insbesondere beim Einsatz von behörden- und verfahrensübergreifenden Verschlüsselungslösungen und dem Virenschutz beim Datenaustausch über das Berliner Landesnetz.

Ein weiterer Schwerpunkt der Arbeitsgruppe IT-Sicherheit war die Fortschreibung der *IT-Sicherheitsstandards* für die Berliner Verwaltung, die eine genauere Ausprägung der in der IT-Sicherheitsrichtlinie definierten Regelungen enthalten. Wesentliche Neuerungen bzw. Änderungen betreffen die Anforderungen an Verschlüsselungsalgorithmen und die Verbindung zu Fremdnetzen. Die IT-Sicherheitsstandards fordern den unbedingten Einsatz von *Verschlüsselungsverfahren* bei der Übertragung von Informationen, die hinsichtlich der Vertraulichkeit, der Nachweisbarkeit und der Integrität besonderen Sicherheitsanforderungen unterliegen. Die eingesetzten Verfahren müssen dem Stand

[45] JB 1995, 4.1; JB 1997, 2.3; JB 1998, 2.2

der Technik entsprechen, dieses sind derzeit Verschlüsselungsalgorithmen wie Triple-DES oder IDEA. Die zur Verschlüsselung verwendeten Produkte dürfen keine Möglichkeiten der Schlüsselaufdeckung enthalten, die einen unbefugten Zugriff Dritter auf die verschlüsselten Daten ermöglicht („Key Escrow“[46]).

Obwohl zwischen der Senatsverwaltung für Inneres, dem IT-KAB und dem Landesbetrieb für Informationstechnik von Anfang an Einigkeit darüber herrschte, dass die Übertragung personenbezogener Daten auf dem Berliner Landesnetz grundsätzlich verschlüsselt werden sollte, haben allerdings praktische Probleme bei der Auswahl eines geeigneten Verfahrens zu erheblichen Verzögerungen bei der Umsetzung dieses Plans geführt. Im Berichtsjahr scheint die Suche nach einem geeigneten Verschlüsselungsverfahren von Erfolg gekrönt worden zu sein[47].

Auch für die Anbindung an *Fremdnetze* wurden Festlegungen getroffen, die wir schon seit mehreren Jahren fordern. Eine Verbindung zu Fremdnetzen setzt voraus, dass einerseits ein schlüssiges Sicherheitskonzept vorliegt, und andererseits, dass dieses auch konsequent umgesetzt wird. Fremdnetze sind alle IT- und TK-Netzinfrastrukturen außerhalb des Geltungsbereiches der IT-Sicherheitsrichtlinie des Landes Berlin wie z. B. Internet, Firmennetze, Verbundnetze wie TESTA, IVBB, Netze von TK-Carriern und Internet-Service-Provider, Mehrwertdienste wie X.25, X.400 und X.500 oder auch das Stadtinformationssystem „Berlin.de“.

Zusammenfassend kann man feststellen, dass die IT-Sicherheitsstandards nunmehr viele verbindliche Festlegungen von Sicherheitsmaßnahmen definieren, die wir bereits seit mehreren Jahren empfehlen.

---

46 JB 1996, 3.4
47 vgl. 4.8.2

3. Schwerpunkte im Berichtsjahr

Zwei Themen, die im vergangenen Jahr einen wichtigen Stellenwert in der politischen Diskussion einnahmen, werfen ein Schlaglicht auf ein Grundproblem, mit dem sich unser Gemeinwesen derzeit konfrontiert sieht:

Auf der einen Seite trägt die jahrzehntelang weltweit geführte Diskussion über die Transparenz staatlicher Entscheidungsprozesse auch in Deutschland späte Früchte. Berlin hat nach Brandenburg als zweites Bundesland nunmehr ein Informationsfreiheitsgesetz, das den Bürgerinnen und Bürgern, ohne dass sie einen Nachweis ihres Interesses erbringen müssten, Zugang zu den Unterlagen der Berliner Verwaltung gewährt, freilich nur soweit, wie gegenläufige Interessen, allen voran der Datenschutz, nicht entgegenstehen.

Andererseits werden immer heftiger Forderungen laut, durch einen zunehmenden Einsatz von Videotechnik die Überwachung der Bürgerinnen und Bürger zu intensivieren. Man verbindet damit die Hoffnung, tatsächlich bestehende oder nur vermeintliche Sicherheitsrisiken beherrschbar zu machen.

3.1. Informationsfreiheit

Der Bericht über die Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten, den der erste Beauftragte Hans-Joachim Kerkau vor nahezu genau 20 Jahren vorlegte, schließt mit folgendem Absatz:

„Schließlich wird der Datenschutz zunehmend im Zusammenhang mit der Frage zu sehen sein, ob sich die öffentliche Verwaltung nicht durch Gewährung eines generellen *Akteneinsichtsrechtes* die für ein demokratisches Gemeinwesen angemessene Transparenz verschaffen sollte[48].“

Trotz des bei oberflächlicher Betrachtung bestehenden Gegensatzes zwischen Datenschutz und Aktenöffentlichkeit war also der Zugang zu Informationen von Anfang an ein Prinzip, das den Datenschutz als Garant der informationellen Selbstbestimmung nicht nur ergänzen, sondern gleichberechtigt neben ihn treten sollte. Die Fragestellung ist immer noch aktuell: „Data Protection and *Freedom of Information:* Two Sides of the Same Coin“ (ohne Fragezeichen) war das Thema einer Sitzung der 21. Internationalen Konferenz der Datenschutzbeauftragten im September vergangenen Jahres in Hong Kong.

Die politische Grundidee für die *Informationsfreiheit* entstammt (ebenso wie der Datenschutzgedanke) der demokratischen Aufbruchsstimmung Anfang der 60er Jahre in den USA. Lange vor der Daten-

48 JB 1979, 5.2

schutzgesetzgebung wurde ein Informationsfreiheitsgesetz für die amerikanische Bundesregierung geschaffen.[49] Entsprechende Gesetze wurden auch in anderen Demokratien verabschiedet[50]. Obwohl die allgemeine Zielsetzung, die staatliche Entscheidungsfindung transparenter zu machen, auch in der Bundesrepublik in der Regel akzeptiert wurde, sah man keinen Anlass, von dem althergebrachten Prinzip der grundsätzlichen Wahrung des Amtsgeheimnisses („Arkan-Prinzip") abzuweichen.

In den öffentlichen politischen Debatten in Berlin ist das Thema in der Vergangenheit immer wieder aufgegriffen worden. So vertrat im Sommer 1980 der Vorsitzende der Gesellschaft für Zukunftsforschung auf einem öffentlichen Seminar in Berlin die Auffassung, der Konflikt zwischen denen, die Amtswissen haben und an den Schalthebeln der Macht sitzen, und denen, die ausgeschlossen sind, sei künftig ein entscheidenderes Existenzproblem als etwa die Umweltkrise oder die strukturelle Arbeitslosigkeit. Die demokratische Regierungsform der Zukunft müsse so gestaltet sein, dass sie von der Gesamtheit der Bürger akzeptiert werden könne[51]. Im Sommer 1990 wurde in das Abgeordnetenhaus (und die Stadtverordnetenversammlung) erstmals ein Gesetz zur Förderung der Informationsfreiheit eingebracht, das allerdings kurz vor dem Ende der Legislaturperiode scheiterte. Fast erneut zehn Jahre später trat in Berlin am 30. Oktober 1999 das Gesetz zur Förderung der Informationsfreiheit im Land Berlin (IFG)[52] in Kraft. Als zweites Bundesland nach Brandenburg hat Berlin damit den Anschluss an die Entwicklung in den anderen großen Demokratien gefunden.

Das Berliner Informationsfreiheitsgesetz gewährt jedem Menschen gegenüber allen öffentlichen Stellen des Landes das Recht auf Einsicht in oder Auskunft über den Inhalt der dort vorhandenen Akten, ohne dass eine persönliche Betroffenheit vorliegen muss. Ausdrücklich können auch juristische Personen, z. B. Wirtschaftsunternehmen, von diesem Recht Gebrauch machen. Diese dürfen die Daten allerdings nicht gewerblich nutzen. Der Informationszugang soll ausdrücklich der demokratischen Meinungs- und Willensbildung sowie der Kontrolle des staatlichen Handelns dienen.

Zwischen den Prinzipien der Informationsfreiheit und des Datenschutzes besteht ein natürliches Spannungsverhältnis: Enthalten die Unterlagen personenbezogene Daten, würden diese mit der Akteneinsicht- oder -auskunft Dritten gegenüber offenbart. Das ist nach den datenschutzrechtlichen Bestimmungen nur dann zulässig, wenn hierfür eine ausdrückliche Rechtsgrundlage vorhanden ist. Das IFG nimmt zu

---

49 Freedom of Information Act von 1967 – neu gefasst 1982

50 z. B. Frankreich: Gesetz Nr. 78–753 v. 1978, Titel 1: Freier Zugang zu Verwaltungsdokumenten; Niederlande: Gesetz über den Zugang der Öffentlichkeit zu der von der Regierung vorliegenden Information v. 1991

51 Tagesspiegel v. 15. 6. 1980

52 GVBl. S. 561

Gunsten der Informationsfreiheit eine neue Gewichtung vor: Nunmehr können auch einzelne Angaben oder auch Listen über bestimmte Personengruppen wie Beteiligte an Verwaltungsverfahren, Eigentümer oder Gutachter herausgegeben werden, wenn sich die Angaben auf Namen, Geburtsdatum, Beruf, Anschrift und Rufnummer beschränken (insoweit geht das Berliner Gesetz deutlich über das brandenburgische hinaus). Angaben über die Mitwirkung von Amtsträgern an Verwaltungsvorgängen sind ebenfalls nicht geschützt. Darüber hinaus können die Behörden personenbezogene Daten offenbaren, wenn sie das Informationsinteresse höher einschätzen als die schutzwürdigen Belange der Betroffenen. In diesem Fall sind die Betroffenen allerdings vor der Herausgabe zu beteiligen. Ausgeschlossen ist die Herausgabe personenbezogener Daten, wenn die Akteneinsicht oder die Auskunft überwiegend aus privaten Gründen begehrt wird, etwa aus Neugier oder um anderen zu schaden.

Der Berliner Datenschutzbeauftragte erhält durch das Gesetz wie in Brandenburg nach dem Vorbild der Regelung in einigen kanadischen Provinzen[53] eine neue Funktion: Bestehen Meinungsverschiedenheiten über die Verpflichtung, den Informationszugang zu gewähren, kann der Berliner Datenschutzbeauftragte angerufen werden, der dann eine Empfehlung ausspricht. Wie beim Datenschutzgesetz kann er allerdings keine Weisungen erteilen. Wegen dieser neuen Funktion trägt der Berliner Datenschutzbeauftragte nunmehr die Amtsbezeichnung „Berliner Beauftragter für den Datenschutz und für das Recht auf Akteneinsicht".

Naturgemäß konnten in den zwei Monaten des vergangenen Jahres, in denen das Gesetz in Kraft war, nur wenige Erfahrungen gesammelt werden. Die Senatsverwaltung für Inneres hat in Abstimmung mit uns Hinweise erarbeitet, die den Verwaltungen helfen sollen, das im Detail nicht einfach zu handhabende Gesetz zu vollziehen[54]. Entgegen den im Gesetzgebungsverfahren geäußerten Befürchtungen ist es jedenfalls nicht zu nennenswerten Beeinträchtigungen der Berliner Verwaltung gekommen.

3.2 Videoüberwachung: Allheilmittel oder Gift für die Freiheitsrechte?

Heftige Debatten gibt es zunehmend über den Einsatz einer Technik, die von der Datenschutzgesetzgebung bisher nur sehr unbefriedigend erfasst ist, obwohl ihr Einsatz mit tief greifenden Eingriffen in die informationelle Selbstbestimmung verbunden ist: der *Videotechnik*.

Diese Technik hat in jüngster Zeit eine rasante Entwicklung genommen. Die Kameras werden immer kleiner und damit für eine verdeckte Überwachung zunehmend tauglicher, die Miniaturisierung geht einher

[53] z. B. in British Columbia: Freedom of Information and Protection of Privacy Act v. 1993
[54] Erste Hinweise zur Anwendung des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin v. 16. 11. 1999, IA 1-0201/48

mit einer Verbesserung der Leistungsfähigkeit (Auflösungsvermögen, ferngesteuerte Zoom- und Schwenkfunktionen, Sichtbarmachung von Infrarotsignalen). Zur Darstellung der von mehreren Kameras aufgenommenen Bilder kann eine Fenstertechnik genutzt werden, die es gestattet, die Anzahl von Monitoren zu reduzieren. Mit der Digitalisierung der Bilder haben sich Speichertechniken entwickelt, die durch Datenkomprimierung und Differenzspeicherung bei bewegten Bildern eine wesentlich höhere Auslastung der verfügbaren Speicherkapazität erlauben. Als nächste Entwicklungsstufe stehen leistungsfähige Systeme zur Videoüberwachung mit integrierter *Bilderkennung* (z. B. der Gesichtserkennung auf biometrischer Basis)[55] ins Haus.

Diese Verbesserungen der Technik, verbunden auch hier mit einem Preisverfall, tragen bei öffentlichen und nicht-öffentlichen Stellen zum Wunsch bei, diese Technik verstärkt für die verschiedensten Überwachungszwecke einzusetzen. Beispiele aus dem vergangenen Jahr sind:

Innenpolitiker fordern immer stärker, *öffentliche Räume,* insbesondere besonders *gefährdete Objekte* flächendeckend mit Videotechnik zur Verhinderung bzw. Verfolgung von Straftaten und Ordnungswidrigkeiten zu überwachen. In der Koalitionsvereinbarung zwischen SPD und CDU zur laufenden Legislaturperiode wurde eine Vereinbarung getroffen, nach der in zurückhaltender Weise an Kriminalitätsschwerpunkten in Berlin Videotechnik eingesetzt werden soll. Ob und inwieweit hierzu das *ASOG* geändert werden muss, wird im laufenden Jahr zu erörtern sein.

Nachdem die *Berliner Verkehrsbetriebe* (BVG) bereits seit einiger Zeit Bahnhöfe, Durchgangstunnel und Vorplätze der U-Bahn mit Videoanlagen überwachen, wurde Ende 1999 ein Pilotprojekt in den Fahrzeugen selbst (Busse, Straßenbahnen, U-Bahnen) gestartet, um die kostenintensiven Vandalismusschäden zu reduzieren. Der jedenfalls bei Bussen und S-Bahnen positiv verlaufene technische Versuch wurde Anfang des neuen Jahres in einen großflächigeren Feldversuch überführt.

Auch andere öffentliche Einrichtungen denken darüber nach, Straftaten oder Hausrechtsverletzungen durch Installation von Überwachungssystemen entgegenzuwirken. Vorschläge, in Eingängen und Höfen von *Schulen* Videokameras einzubauen, haben zu einer heftigen Debatte darüber geführt, ob die Aufsicht durch die Lehrer durch Technik ersetzt werden kann. Die Kindesentführung aus der Säuglingsstation einer Berliner Klinik Ende September 1999 hat eine öffentliche Diskussion über den Einsatz in *Kliniken* entfacht. Die Gesundheitssenatorin hat sich allerdings geweigert, alle Neugeborenenstationen entsprechend auszurüsten.

---

[55] JB 1998, 3.5

Noch stärker ist der Drang, Videotechnik in privaten Einrichtungen einzusetzen. Der Einsatz von Videoüberwachungssystemen in *Kaufhäusern* und *Supermärkten* gehört mittlerweile schon zum Alltag. Auch andere Geschäfte gehen zunehmend dazu über, ihre Verkaufsräume mit derartigen Anlagen zu überwachen, um Ladendiebe abzuschrecken bzw. zu verfolgen. So gibt es kaum noch Tankstellen, die sich nicht dieser Technik bedienen.

Banken überwachen zumindest die Räume, in denen Serviceautomaten, insbesondere Geldautomaten aufgestellt sind. Zur Vermeidung von Vandalismusschäden tritt hier das Bedürfnis hinzu, missbräuchliche Benutzung zu verhindern bzw. Beweismittel für die Inanspruchnahme der Automaten zu sammeln.

Das 3-S-Konzept der *Deutschen Bahn*[56] besteht im Wesentlichen aus einer Videoüberwachung der Fern- und S-Bahnhöfe. Der Einsatz von Videotechnik in den Zügen selbst ist geplant.

Gespalten ist die Meinung von Mietern darüber, ob der Einsatz der Videotechnik zur Überwachung des Wohnumfeldes (Eingangsbereiche, Spielplätze, Stellflächen für Abfallentsorgung) eine Verbesserung der Wohnqualität darstellt oder doch eine beeinträchtigende Überwachung der *Mieter* durch den Vermieter oder den Hausmeister darstellt. In einer Wohnanlage haben die Mieter sogar zugestimmt, die von einer Videokamera auf dem Kinderspielplatz der Anlage aufgenommenen Bilder in das TV-Kabelnetz einzuspielen.

Zunehmend mehr überwachen Arbeitgeber *Arbeitnehmer* mit Videotechnik trotz der restriktiven Rechtsprechung der Arbeitsgerichte[57].

Während es sich bei all diesen Beispielen um interne, für abgrenzbare Zwecke bestimmte Anwendungen handelt, zeichnen sich Entwicklungen ab, die einer derartigen Zweckbindung nicht mehr unterliegen: Mit Hilfe von *Webcams* können Bilder über das Internet in der ganzen Welt verbreitet werden. Aus spielerischen Anwendungen wie z. B. zur Beobachtung des Füllstandes studentischer Kaffeemaschinen oder des Baufortschritts am Potsdamer Platz können schnelle diskriminierende oder zu Straftaten einladende Bilder werden.

Dass es offensichtlich Leute gibt, die durch derartige Webcams jedem Menschen in der Welt Einblick selbst in das *Intimleben* gestatten, deutet darauf hin, dass in der Tat das Bewusstsein über den Wert der Privatssphäre nicht überall hinreichend entwickelt ist[58]. Noch erschreckender ist, dass derartige Übertragungen sogar Zuschauerrekorde erzielen können, wenn Fernsehanstalten (wie im Projekt „Big Brother“ in den Niederlanden) derartige Dinge bewusst in Szene setzen.

---

56 vgl. 4.6.3
57 vgl. 4.3.1
58 JB 1998, Einleitung

3.2

Dass auch Erwartungen bestehen, mit der Verbreitung von Videoaufnahmen kommerziellen Erfolg zu erzielen, zeigen die umstrittenen Aktivitäten einer Firma, die unter der Bezeichnung *„CityServer“* eine *Bilderdatenbank* von Häusern und Gebäuden aller deutschen Städte mit mehr als 20 000 Einwohnern vertreiben will[59].

Dass es sich bei all diesen Anwendungen um einen Eingriff in Persönlichkeitsrechte handelt, bedarf keiner Diskussion. Mit hinreichender Deutlichkeit hat das Bundesverfassungsgericht zum Recht am eigenen Bild und gesprochenen Wort ausgeführt: „Jedermann darf grundsätzlich selbst und allein bestimmen, ob und wieweit andere sein Lebensbild im Ganzen oder bestimmte Vorgänge aus seinem Leben öffentlich darstellen dürfen“[60]. Aus der Rechtsprechung zur informationellen Selbstbestimmung muss gefolgert werden, dass dieses Recht nicht nur die öffentliche Darstellung, sondern bereits die Erhebung der entsprechenden Daten umfasst.

Trotz dieser klaren grundrechtlichen Ausgangslage sind die bestehenden Gesetze äußerst unbefriedigend.

Spezielle Regelungen zum Einsatz der Videotechnik bestehen im öffentlichen Bereich nur zur Untersuchung einer (konkreten) Straftat von erheblicher Bedeutung (§ 100 c StPO), zur Verhütung einer Straftat von erheblicher Bedeutung (§ 25 Abs. 1 ASOG), zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person (§ 25 Abs. 4 ASOG) sowie bei erheblichen Gefahren für die öffentliche Sicherheit und Ordnung anlässlich öffentlicher Versammlungen (§ 13 a Versammlungsgesetz). Für den Einsatz der Videotechnik durch Privatunternehmen und -personen fehlt jegliche rechtliche Regelung.

Auch die Datenschutzgesetze ermöglichen keine klare Entscheidung über die Zulässigkeit des Einsatzes der Videotechnik. Im nicht-öffentlichen Bereich werden Videoaufnahmen bereits terminologisch aus dem Geltungsbereich des Bundesdatenschutzgesetzes herausgenommen (§ 3 Abs. 3 BDSG). Die bei digitalen Aufnahmen prinzipiell mögliche automatische Auswertbarkeit der Aufnahmen, die zu einer Geltung des BDSG führen würde, ist in aller Regel nicht gegeben. Zwar gilt diese Einschränkung für die Behörden des Bundes und der Länder nicht, konkrete Regelungen für die Videotechnik fehlen allerdings sowohl im Bund als auch in Berlin. Während die Bundesverwaltung auf die Generalklauseln des BDSG zurückgreifen kann, die eine Erhebung und Verarbeitung von Daten zulassen, soweit dies für die Aufgabenerfüllung erforderlich ist, ist dieser Weg in Berlin versperrt, da nach dem Berliner Datenschutzgesetz eine ausdrückliche Rechtsgrundlage erforderlich wäre. Lediglich für die Ausübung des *Hausrechtes* können allgemeine zivilrechtliche Prinzipien herangezogen werden.

---

59 vgl. 4.6.4

60 BVerfGE 35, 202 (220) – Lebach –

Wegen dieser Situation muss bei der rechtlichen Beurteilung der Videotechnik von folgenden allgemeinen Prinzipen ausgegangen werden, die für den öffentlichen und privaten Bereich gleichermaßen gelten:

Dient die Videotechnik lediglich der *Beobachtung* von Räumen, die ebenso gut von einem Menschen (z. B. einem Polizisten, einem Kaufhausdetektiv oder einem Hausmeister) beobachtet werden könnten, ist der Einsatz der Videotechnik zulässig, soweit er im Rahmen der Aufgabenerfüllung, der Vertragsabwicklung oder der Wahrnehmung des Hausrechtes angemessen ist. Da eine verdeckte Videoüberwachung einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte darstellen würde, ist über den Kameraeinsatz zu informieren, was in der Regel durch entsprechende *Hinweisschilder* erfolgt.

Erheblich höhere Anforderungen sind an die Rechtmäßigkeit der *Aufzeichnung* zu stellen. Da hier, außer in den angegebenen Fällen, eine ausdrückliche Rechtsgrundlage fehlt, sind Aufnahmen nur dann zulässig, wenn eine Straftat beobachtet wird oder eine konkrete Gefahrenlage besteht. Nur im Einzelfall kann davon ausgegangen werden, dass eine derartige Gefahr permanent herrscht und daher eine anlasslose Aufzeichnung zulässig ist (z. B. bei Geldautomaten). Aber auch hier sind die Betroffenen aufzuklären. Strenge Anforderungen müssen an die Nutzung der Aufzeichnungen gestellt werden, die nur verwertet werden dürfen, wenn dies zur Zweckerfüllung unerlässlich ist.

Für die Beobachtung *öffentlich zugänglicher Räume* sieht das künftige BDSG eine Rechtsgrundlage für die Videoüberwachung vor, soweit diese zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Wenn dies zum Erreichen des verfolgten Zweckes erforderlich ist, soll auch die Speicherung zulässig sein.

Auch diese Entwurfsfassung wird den Risiken der Videotechnik nicht gerecht. Insbesondere müssen klarere Kriterien herausgearbeitet werden, in welchen Fällen über die Beobachtung hinaus eine Aufzeichnung zulässig sein soll. Beschränkt sich die Voraussetzung, so wie der Entwurf dies vorsieht, auf die Erforderlichkeit für die Zweckerfüllung, gibt es keine hinreichend scharfe Trennung der Befugnisse zur Beobachtung und zur Speicherung mehr. Vielmehr muss daran festgehalten werden, dass die Speicherung eines konkreten, über den allgemeinen Zweck hinausgehenden Anlasses bedarf.

Verhindert werden muss eine flächendeckende Videoüberwachung öffentlicher Räume: Das Grundrecht auf Freizügigkeit (Art. 11 GG) gewährt nicht nur die Möglichkeit, sich frei zu bewegen, sondern auch, dass dies nicht festgehalten und später den Grundrechtsträgern entgegengehalten wird.

3.2

Erstaunlich ist angesichts der Risiken, dass Umfragen in der Bevölkerung eine hohe Akzeptanz der Videotechnik ergeben haben[61]. Dabei ist es umso überraschender, dass der Anteil der Befürworter der Videoüberwachung unter den Bürgerinnen und Bürgern der ehemaligen DDR besonders hoch ist. Aber aus den Befragungen ergibt sich sehr deutlich, dass das subjektiv wahrgenommene Sicherheitsgefühl die Wahrnehmung der persönlichkeitsrechtlichen Einschränkungen, die mit derartigen Maßnahmen verbunden sind, (noch) bei weitem überwiegt. Jedenfalls bei der Überwachung öffentlicher Räume wird möglicherweise nur vorübergehend eine Verbesserung der Sicherheitslage erreicht. Erfahrungen aus Großbritannien, wo die Überwachungssysteme bereits eine ganz andere Dimension als in Deutschland erreichen, aber auch die als modellhaft gepriesene Überwachung des Vorplatzes am Hauptbahnhof in Leipzig haben gezeigt, dass selbst großflächig angelegte Maßnahmen nicht dauerhaft greifen. Zum einen ist eine – zeitweise – Verlagerung krimineller Aktivitäten in andere Bereiche feststellbar, zum anderen setzt die Wirksamkeit eine schnelle Reaktion voraus. Dies ist allenfalls bei der Konzentration auf bestimmte Orte, keinesfalls aber bei flächendeckendem Einsatz möglich.

---

61 Berliner Morgenpost v. 25. 7. 1999, S. 1

4. Aus den Arbeitsgebieten

4.1 Sicherheit

4.1.1 Verfassungsschutz

Das „Abhör-Urteil“ des Bundesverfassungsgerichtes

Das Bundesverfassungsgericht hat in seinem Urteil vom 14. Juli 1999[62] zum Verbrechensbekämpfungsgesetz 1994[63] die verdachtslose Überwachung, Aufzeichnung und Auswertung internationaler Fernmeldeverkehrsbeziehungen nach bestimmten Suchworten zur Früherkennung von aus dem Ausland drohenden schweren Gefahren durch den Bundesnachrichtendienst grundsätzlich für zulässig erklärt. Das Bundesverfassungsgericht hat leider nicht den „Stecker des elektronischen Staubsaugers“ herausgezogen und für eine klare Trennung zwischen Geheimdiensten und Polizei gesorgt. Es hat aber für die *Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen* wurden, deutliche Schranken gezogen, die weit über das Urteil hinaus bedeutsam sind.

Für die Behörden, die rechtmäßig Telekommunikation überwachen dürfen und zu denen das Berliner Landesamt für Verfassungsschutz gehört, ergeben sich daraus ganz konkrete Konsequenzen:

Zur Sicherung der *Zweckbindung* und um eine Kontrolle der Verwendung der erlangten Daten zu ermöglichen, muss auch nach der Erfassung erkennbar bleiben, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende *Kennzeichnung* bei der erhebenden Stelle und bei den Übermittlungsempfängern ist daher geboten.

Konsequenzen hat das Urteil auch für die *Benachrichtigung der Betroffenen.* Nicht nur bei Eingriffen in das Fernmeldegeheimnis ist dies Voraussetzung dafür, dass der Betroffene von den ihm zustehenden Rechten Gebrauch machen kann, und daher von Art. 19 Abs. 4 GG geboten. Formale Kriterien, wie bestimmte Speicherfristen, können die Unterrichtungspflicht nicht aufheben. Damit ist § 9 Abs. 5 LfVG nicht zu vereinbaren, wonach eine Unterrichtung des Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.

Nicht erforderliche Daten, die durch einen Eingriff in das Fernmeldegeheimnis erlangt wurden, müssen unverzüglich *gelöscht* werden – es sei denn, der Rechtsschutz des Betroffenen würde dadurch verkürzt. Die Haltung des LfV, nicht (mehr) erforderliche Daten, wenn sie sich in

---

62 Urteil v. 14. 7. 1999, Az.: BvR 2226/94, 2420/95 und 2437/95; vgl. auch 1.1
63 JB 1994, 4.8

Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden.

Die *Vernichtungspflicht* ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz des Betroffenen zu vereiteln. Eine Löschung oder Vernichtung personenbezogener Daten nach der Stellung eines Auskunftsantrages ist damit unzulässig.

Die *Kontrolllücke* bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden[64], ist verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet. Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken. Das Ausführungsgesetz zum G 10 (AG G 10) ist nicht bestimmt genug. Es ist klarzustellen, ob die G 10-Kommission auch für die Kontrolle der weiter gehenden Datenverarbeitung zuständig ist oder ob die Kontrolle vom Berliner Beauftragten für Datenschutz und Akteneinsicht wahrzunehmen ist. Das Bundesverfassungsgericht hat gefordert, dass auch im Bereich der Landesverwaltung eine ausreichende Kontrolle existieren muss. Unabhängig von der Klarstellung im Gesetz ist im Vorgriff ein gangbarer Weg für die Praxis bei Datenschutzprüfungen zu vereinbaren.

4.1.2 Polizei

Neue Befugnisse

Das Allgemeine Sicherheits- und Ordnungsgesetz (*ASOG*) wurde in einigen datenschutzrechtlich bedeutsamen Punkten geändert[65].

Die Regelungen zum *Großen Lauschangriff* mussten den Änderungen des Art. 13 GG[66] angepasst werden. Die Möglichkeiten des Einsatzes dieser Maßnahme in öffentlich zugänglichen Arbeits-, Betriebs- und Geschäftsräumen wurden beschränkt, das Abhören in Wohnungen zum Schutz einer bei einem polizeilichen Einsatz tätigen Person bedarf nunmehr der Anordnung eines Beamten des höheren Dienstes, und die erlangten Erkenntnisse unterliegen jetzt besonderen Verwendungsregelungen. Weiterhin wird – im Gegensatz zu den Lauschangriffen zur Strafverfolgung[67] – eine jährliche Berichtspflicht gegenüber dem Abgeordnetenhaus gesetzlich vorgeschrieben.

---

64 JB 1996, 4.1.2
65 Gesetz zur Änderung des ASOG v. 11. 5. 1999, GVBl. S. 164
66 JB 1998, 1.1
67 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern“, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A II, vgl. 4.3.1

Statt der kritischen Überprüfung der langen polizeilichen Speicherfristen[68] wurde bei dieser Gelegenheit kurzerhand § 43 Abs. 3 ASOG gestrichen, wonach die Betroffenen, deren Daten länger als fünf Jahre in automatischen Dateien gespeichert sind, hiervon zu unterrichten sind. Die Streichung dieser *Unterrichtungspflicht* ist nur hinnehmbar, wenn gleichzeitig kürzere Löschungs- und Prüffristen vorgesehen werden. Unsere konkreten Vorschläge hierzu wurden jedoch noch nicht aufgegriffen.

Ein weiteres Instrument der verdachts- und anlassunabhängigen Kontrolle, die *Schleierfahndung,* wurde eingeführt. Zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität kann die Polizei nunmehr „im öffentlichen Verkehrsraum" angetroffene Personen kurzzeitig anhalten, befragen und verlangen, dass mitgeführte Ausweispapiere zur Prüfung angehändigt werden, sowie mitgeführte Sachen in Augenschein nehmen (§ 18 Abs. 7 ASOG).

Die herkömmlichen Bestimmungen des Rechts der Strafverfolgung und der Gefahrenabwehr sind darauf ausgerichtet, dass Eingriffe durch die Polizei zureichende tatsächliche Anhaltspunkte für das Vorliegen einer Straftat bzw. eine konkrete Gefahr voraussetzen. Dieses grundlegende persönliche Zurechnungskriterium des Polizeirechts wird bei den verdachtsunabhängigen Kontrollen aufgegeben. Der Eingriff kann auch gegen Unbeteiligte und Nichtverantwortliche erfolgen. Jeder Bürger kann Ziel einer Kontrolle werden.

Die Berliner Regelung geht über die Befugnisse nach dem Bundesgrenzschutzgesetz und anderen Landesgesetzen noch hinaus. Während der BGS derartige Kontrollen auf Züge, Bahn- und Luftverkehrsanlagen und z. B. die bayerische Polizei auf das Grenzgebiet sowie Durchgangsstraßen (Bundesautobahnen, Europastraßen u. a. Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr) zu begrenzen hat, sollen sich die Befugnisse der Berliner Polizei auf den gesamten „öffentlichen Verkehrsraum" erstrecken. Wenn aufgrund von Lageerkenntnissen anzunehmen ist, dass Straftaten von erheblicher Bedeutung begangen werden sollen, darf im gesamten Berliner Stadtgebiet jeder befragt und seine Ausweispapiere kontrolliert werden. Ort, Zeit und Umfang der Maßnahme werden vom Gesetz offen gelassen und können vom Polizeipräsidenten oder seinem Vertreter bestimmt werden.

Unseren Empfehlungen, die Maßnahme zumindest auf Orte zu begrenzen, die von erheblicher Bedeutung für den grenzüberschreitenden Verkehr sind, eine Höchstfrist von drei Monaten für diese Maßnahme vorzusehen und die mangelnde Transparenz wenigstens durch die Verpflichtung einer Bekanntgabe gegenüber den überprüften Perso-

[68] JB 1998, 3.1

nen abzumildern, wurde nicht gefolgt. Die Bestimmung wurde lediglich um eine Frist von jeweils 14 Tagen ergänzt, nach der zu prüfen ist, ob die Voraussetzungen für die Maßnahme weiterhin vorliegen.

Das *Landesverfassungsgericht Mecklenburg-Vorpommern* hat die Befugnis zu verdachts- und ereignisunabhängigen Kontrollen auf mehr als 30 Kilometer von den Grenzen entfernten Durchgangsstraßen zwischenzeitlich für verfassungswidrig erklärt[69]. Wenn auch die Berliner Regelung (schon wegen des hier fehlenden Grenzgebietes) von der dortigen Regelung abweicht, stellen einige bedeutsame Grundsätze des Urteiles auch die Verfassungsmäßigkeit des ASOG in Frage. So ist auch hier angesichts des Fehlens einer klaren örtlichen Begrenzung zweifelhaft, ob der verfassungsrechtlich notwendige Zurechnungszusammenhang zwischen dem Einzelnen, der kontrolliert wird, und der abzuwendenden Schädigung besteht. Die Bezugnahme auf den weiten Begriff „Straftat von erheblicher Bedeutung", von dem in Berlin sogar Ordnungswidrigkeiten erfasst sind (§ 17 Abs. 4 ASOG), ist zu weit gehend. Es ist ein Straftatenkatalog notwendig, der auf die Begehungsformen der Organisierten Kriminalität zugeschnitten ist.

Das Verfahren zur Ermittlung der Lage, in der die Polizei die Maßnahme ergreifen darf, muss nachvollziehbar sein. Es ist zu dokumentieren, aufgrund welcher Erkenntnisse die Einschätzung gewonnen worden ist, dass bestimmte Straftaten begangen werden sollen, und warum ein hinreichender Grund für die Einbeziehung der jeweiligen Örtlichkeit/Straße besteht.

Regelungen zur Verarbeitung, Nutzung und insbesondere Löschung personenbezogener Daten, die bei den Kontrollen gewonnen werden, sind erforderlich. Der Personenkreis, von dem personenbezogene Daten verwendet werden dürfen, ist festzulegen. Dabei ist zu regeln, welche „Verdachtsschwelle" erreicht sein muss. Bereichsspezifische Vorschriften über die Zweckbindung mit eventuellen Verboten der Weitergabe und Verwertung sind erforderlich.

Mit dem Gesetz über den *Freiwilligen Polizeidienst* (FPDG) vom 11. Mai 1999[70] soll nicht eine Fortsetzung der Freiwilligen Polizeireserve geregelt, sondern ein Freiwilliger Polizeidienst für die neuen Aufgaben Berlins geschaffen werden. Das Gesetz enthält neue Anforderungen für die Aufnahme in den bzw. den Ausschluss vom Freiwilligen Polizeidienst. Unsere Empfehlungen, den Gesetzentwurf um Regelungen zu Art und Umfang der Überprüfung der Bewerber zu ergänzen, klarzustellen, dass die Überprüfung nur mit Einwilligung der Betroffenen erfolgt, und die erforderlichen Datenerhebungen (Vorlage eines Führungszeugnisses, Nutzung des Polizeilichen Informationssystems) zu benennen, sind nicht aufgegriffen worden. Der Innensenator hat

---

69 Urteil v. 21. 10. 1999, Az.: LVerfG 2/98
70 GVBl. S. 165

zugesagt, dass seine Verwaltung bei dem Erlass von Verwaltungsvorschriften dieses Problem aufgreifen wird. Ein Entwurf liegt uns bisher noch nicht vor.

Katastrophen wie Flugunfälle, Unfälle bei Groß- und Massenveranstaltungen oder Schadstoffausbreitungen unterscheiden sich dadurch von den Alltagsgefahren – für deren Bekämpfung mit dem ASOG, Feuerwehrgesetz und Rettungsdienstgesetz ausreichende rechtliche Grundlagen vorhanden sind -, dass sie das Leben und die Gesundheit einer Vielzahl von Menschen oder der Umwelt gefährden und von den Ordnungsbehörden mit eigenen Mitteln und Kräften nicht angemessen beseitigt werden können. Das neue *Katastrophenschutzgesetz* vom 11. Februar 1999[71] regelt nunmehr das Zusammenwirken aller in diesem Fall zu beteiligenden Behörden und der anderen Mitwirkenden wie Anlagenbetreiber oder freiwillige Helfer.

Datenschutzrechtlich zu diskutieren war die Einrichtung einer *Personenauskunftsstelle* bei der Polizei. Die Fassung im Entwurf war nicht hinreichend bestimmt. Weil von den beabsichtigten Übermittlungspflichten auch die ärztliche Schweigepflicht (beispielsweise Auskünfte durch Krankenhausärzte) berührt ist, haben wir empfohlen, konkret zu regeln, welche Daten zur Auskunftserteilung gespeichert werden, welche Daten an die Polizei zu übermitteln sind und an wen Auskünfte zu welchem Zweck zu erteilen sind.

Damit soll nicht der Kreis derjenigen, die Auskünfte über das Schicksal von Personen erhalten, über Gebühr eingeschränkt, sondern lediglich präzisiert werden, wer über die Angehörigen hinaus noch berechtigt sein soll. Die verabschiedete Fassung des Gesetzes entspricht nicht ganz unseren Vorstellungen; allerdings bestand bei den parlamentarischen Beratungen Einvernehmen darüber, dass eine Konkretisierung in den vom Senat angekündigten Ausführungsvorschriften vorgenommen wird.

Konsequenzen aus dem „Abhör-Urteil“

Das Urteil des Bundesverfassungsgerichtes zum Verbrechensbekämpfungsgesetz 1994[72] betrifft nicht nur die *strategische* Überwachung des Fernmeldeverkehrs durch die Nachrichtendienste. In der Entscheidung werden zur Verwendung personenbezogener Daten, die aus *Fernmeldeüberwachungen* gewonnen wurden, Bedingungen formuliert, die auch für die Polizei Bedeutung haben. Diese Bedingungen müssen auch für die Verwendung anderer Daten gelten, die einer besonderen Zweckbindung unterliegen und die durch Maßnahmen erlangt wurden,

71 GVBl. S. 78
72 vgl. 1.1, 4.1.1, 4.3.1

die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, das sind insbesondere das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit Einsatz technischer Mittel, der Große Lauschangriff, der Einsatz verdeckter Ermittler und die polizeiliche Beobachtung.

Personenbezogene Daten, die aus Eingriffen in das Fernmeldegeheimnis stammen, sind künftig auch von der Polizei zur Sicherstellung der Zweckbindung zu *kennzeichnen.* Das gilt für Daten, die die Polizei (z. B. durch Telefonüberwachungsmaßnahmen) selbst erhoben hat, und für Daten, die andere Stellen (z. B. Verfassungsschutzämter oder andere Sicherheitsbehörden) durch einen Eingriff in das Fernmeldegeheimnis erlangt und an die Polizei übermittelt haben.

Die *Benachrichtigung des Betroffenen* darf nur unterbleiben, wenn die erfassten Daten ohne weitere Schritte sogleich als irrelevant vernichtet werden. Dieser Anforderung scheint § 25 Abs. 7 Satz 2 ASOG zu entsprechen. Danach kann die Unterrichtung des Betroffenen unterbleiben, wenn die erlangten personenbezogenen Daten oder hieraus gewonnene Erkenntnisse unverzüglich nach Beendigung der Maßnahme vernichtet worden sind. Bei einer weiteren Speicherung der Daten – auch wenn sie nur aus Gründen der Verwaltungspraktikabilität erfolgt – oder bei jeder weiteren Verwendung der Daten (z. B. durch einen Datenabgleich) ist der Betroffene zu unterrichten.

Nicht erforderliche Daten, die durch einen Eingriff in das Fernmeldegeheimnis erlangt wurden, müssen unverzüglich gelöscht werden – es sei denn, der Rechtsschutz des Betroffenen würde dadurch verkürzt. Die personenbezogenen Daten, die aus diesen Maßnahmen stammen und nicht mehr für die Aufgabenerfüllung erforderlich sind, sind *in den Akten zu schwärzen,* und Unterlagen mit derartigen Erkenntnissen sind unverzüglich aus den Akten zu entfernen und zu vernichten. § 48 Abs. 3 ASOG ist entsprechend zu ändern bzw. zunächst verfassungskonform dahingehend anzuwenden.

Die *Verpflichtung zur Löschung* unzulässig gespeicherter oder nicht mehr erforderlicher Daten ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Maßnahmen sind unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz des Betroffenen zu vereiteln. Eine Löschung oder Vernichtung personenbezogener Daten während eines noch nicht rechtskräftig abgeschlossenen Auskunftsverfahrens ist damit unzulässig. Zudem sind die Daten nach einer Unterrichtung des Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.

Das Bundesverfassungsgericht hat eine hohe Schwelle angesetzt für die *Auswertung* von aus der Fernmeldeüberwachung stammenden Daten durch die erhebende Stelle. Die Verwendung darf nicht zu jedem beliebigen Zweck erfolgen, sondern nur für die Gefahrenfelder, für die

eine Telefonüberwachungsmaßnahme zulässig wäre. Die Daten dürfen – außer für den der Anordnung zugrunde liegenden Zweck oder zur Strafverfolgung – nur für die Verfolgung von Straftaten von erheblicher Bedeutung genutzt werden. § 25 Abs. 8 ASOG ist verfassungskonform entsprechend auszulegen.

Nicht nur die Vernichtung, sondern auch die Übermittlung der Daten, die durch einen Eingriff in das Fernmeldegeheimnis erlangt wurden, ist zu *protokollieren.* Für die Vernichtung der Unterlagen ist dies in § 25 Abs. 8 ASOG bereits vorgesehen. Für die Datenübermittlung ist eine entsprechende Regelung zu schaffen.

Errichtungsanordnungen

Nicht von der Senatsverwaltung für Inneres, sondern von dritter Seite haben uns Entwürfe zu *Errichtungsanordnungen für Analyse-Arbeitsdateien* sowohl auf Bundes- (Fallanalytisches Verfahren und ViCLAS-Datenbanksystem) als auch auf europäischer Ebene erreicht. Damit wird ein völlig neuer Dateityp mit einer beispiellosen Quantität und Qualität der zur Erfassung und Auswertung vorgesehenen Daten geschaffen.

Das beim Bundeskriminalamt (BKA) geplante Verfahren *ViCLAS*[73] dient der Erkennung von Tatzusammenhängen bei Gewaltdelikten, der Täteridentifizierung und Zusammenführung von Serien im Bereich der sexuellen Gewalt und der Tötungsdelikte sowie der Gewinnung von Präventionsansätzen und ermöglicht, die Kriminalitätsentwicklung in bestimmten Delikts- und Tatfeldern (beispielsweise Straftaten gegen Leben, Freiheit und die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung unter Anwendung körperlicher Gewalt, aber auch verdächtiges Ansprechen von Kindern und Jugendlichen, wenn ein sexuelles Gewaltmotiv ermittelt werden kann und nach Sachlage tatsächliche Anhaltspunkte für eine geplante schwerwiegende Straftat vorliegen) zu beobachten. Bei ViCLAS werden alle nach dem BKA-Gesetz denkbaren Möglichkeiten zur Speicherung von Personendaten aufgezählt. Eine Konkretisierung, über welche Personengruppe Daten tatsächlich erforderlich sind, erfolgt nicht.

Das wesentliche Problem liegt in dem beispiellosen *Datenumfang.* Danach sollen detaillierte Merkmalekataloge teilweise aus dem intimsten Bereich nicht nur über den Beschuldigten erfasst werden, sondern auch ohne deren Einwiligung über Opfer und über Vermisste. Das ist bei Opfern in dieser Qualität und Quantität in einer bundesweiten Verbunddatei nicht vertretbar. Auch die personenbezogene Speicherung von Vermisstendaten halten wir wegen der umfassenden Registrierung aus allen denkbaren Lebensumständen unverhältnismäßig.

---

[73] Violent Crime Linkage Analyses System = Analyse-System zur Verknüpfung von Gewaltverbrechen

4.1.2

Zum Zeitpunkt unserer Rückfrage bei der Innenverwaltung war der Entwurf der Errichtungsanordnung dort angeblich noch nicht bekannt. Statt sich mit unseren Einwänden auseinander zu setzen, bestand lediglich ein ausgeprägtes Interesse daran, wer uns den Entwurf zugeleitet hat. Das Verfahren wird seit dem 1. Januar 2000 auch bei der Berliner Polizei eingesetzt, ohne dass unsere Einwände berücksichtigt wurden.

Auch einen Entwurf einer Mustererrichtungsanordnung für *Europol-Analyse-Dateien* halten wir für nicht akzeptabel. Damit wird der durch die Durchführungsbestimmungen für die von Europol geführten Arbeitsdateien zu Analyse-Zwecken[74] eröffnete – ohnehin außerordentlich weit gehende – Rahmen zwar komplett ausgeschöpft, wichtige datenschutzrechtliche Einschränkungen werden jedoch ausgelassen. Die Festlegungen in einem Ankreuz-Verfahren lassen den Eindruck der Beliebigkeit entstehen, die Analysen haben nur noch den Charakter von Brainstormings.

Es wird auch nicht deutlich, ob und mit welcher Zusammensetzung und Aufgabenstellung eine Analyse-Gruppe gebildet werden soll. Das ist nach Art. 10 Abs. 2 Satz 2 Europol-Übereinkommen aber Voraussetzung für die Errichtung einer Analyse-Datei. Es muss eine Begrenzung auf solche Personengruppen vorgenommen werden, die für den Analyse-Zweck tatsächlich relevant sind. Problematisch sind insbesondere die Aufnahme von Zeugen und der Umfang und das mögliche weitere Schicksal der Daten zu diesen Personen. Da die Ereignisse, die zu Datenspeicherungen führen können, nicht definiert sind, fehlen Anhaltspunkte für den Fristbeginn.

Auch dieser Musterentwurf hat der Senatsverwaltung für Inneres zum Zeitpunkt unserer Anfrage noch nicht vorgelegen. Weil in Art. 12 Abs. 1 des Europol-Übereinkommens eine Zustimmung oder auch eine Mitwirkung der Bundesländer nicht vorgesehen ist, besteht dort auch nicht die Absicht, sich inhaltlich zu dem Problem zu äußern, obwohl es sich um Daten handelt, die von den Ländern in die Verbunddatei bei dem BKA eingestellt wurden. Bisher hat der Polizeipräsident allerdings an keinem der Analyse-Projekte bei Europol teilgenommen und auch keine personenbezogenen Daten unmittelbar hierfür übermittelt.

Die Senatsverwaltung für Inneres hat uns sehr zeitig den Entwurf einer Errichtungsanordnung für eine *Geldwäschedatei* als Verbunddatei beim Bundeskriminalamt übersandt, mit der geldwäscherelevant erscheinende Sachverhalte aufgrund von Geldwäsche-Verdachtsanzeigen verarbeitet werden sollen.

Geldwäsche-Anzeigen werden durch gesetzliche Mitteilungspflichten der Banken ausgelöst, die mit Strafanzeigen aufgrund von Beobachtung von Straftaten oder eigener Betroffenheit nicht vergleichbar sind.

---

74 ABlEG C 26/1

Den Anzeigen fehlt die Qualität, die erforderlich ist, um die im BKAG geforderten Negativ-Prognosen begründen zu können. Darüber hinaus fehlt es häufig an der für die Speicherung in der Verbunddatei wesentlichen überregionalen Bedeutung oder Schwere. Im Übrigen bietet bereits das Zentrale Staatsanwaltschaftliche Verfahrensregister die Möglichkeit, die aufgrund eines hinreichenden Anfangsverdachtes gegen einzelne Beschuldigte eingeleiteten Ermittlungsverfahren bundesweit zu speichern.

Speicherungen in der Datei sollen auch hier nicht auf Personen begrenzt bleiben, gegen die ein konkreter Tatverdacht besteht. Mit der Erweiterung auf den Kreis der Verdächtigen werden Personen einbezogen, gegen die nicht mehr vorliegt als die Annahme eines nach dem Geldwäschegesetz anzeigeverpflichteten Institutes, es könnte sich vielleicht um Geldwäsche handeln.

In Berlin führen Geldwäsche-Anzeigen regelmäßig zur Einleitung von Ermittlungsverfahren, die allerdings überwiegend wieder eingestellt werden. Die Betroffenen haben zunächst den Status eines „Beschuldigten". Die Senatsverwaltung für Inneres vertritt die Auffassung, dass eine Speicherung nach § 8 Abs. 1 BKAG zulässig sei, weil diese Vorschrift nur an die formale Beschuldigten-Eigenschaft anknüpft, ohne dass die Daten verarbeitende Stelle eine Prüfung vorzunehmen hätte, ob das Ermittlungsverfahren zu Recht eingeleitet wurde. Auch die Speicherung der Verdächtigen hält sie für unbedenklich, weil die Errichtungsanordnung lediglich eine generell abstrakte, enumerative Aufzählung der Daten enthält, die für eine Speicherung in der Datei in Betracht kommen. Die Errichtungsanordnung kann demgegenüber gesetzliche Speicherungsbefugnisse weder ersetzen noch erweitern. Deshalb muss in jedem Einzelfall geprüft werden, ob die Voraussetzungen des § 8 Abs. 2 bis 4 BKAG vorliegen. Immerhin wird eingeräumt, dass die erforderlichen Prognosen in vielen Fällen nicht gestellt werden können und eine Datenspeicherung daran scheitert.

Keine Verbesserung bei Kriminalakten

Einer der Schwerpunkte im vergangenen Berichtsjahr[75] war die nach bestimmten Fristen vorzunehmende Prüfung, ob für die Polizei die in *Kriminalakten* und im Informationssystem Verbrechensbekämpfung (ISVB) gespeicherten Daten zur ordnungsgemäßen Aufgabenerfüllung noch erforderlich sind oder gelöscht werden müssen. Wir haben zur Optimierung des Verfahrens und zur Verbesserung des Datenschutzes verschiedene Anregungen und Empfehlungen gegeben, denen der Polizeipräsident in Berlin fast durchgängig nicht folgen will.

75 JB 1998, 3.1

4.1.2

In den Kriminalakten werden Unterlagen zu *Vermissten- und Suizid-Vorgängen* mit der Begründung abgelegt, dass diese *kriminalpolizeilichen Personenakten* sämtliche Erkenntnisse enthalten müssen, die der vorbeugenden Verbrechensbekämpfung dienen. Dabei wird verkannt, dass es sich hier um Daten handelt, die zu unterschiedlichen Zwecken gespeichert werden. Die Vermissten- und Suizid-Vorgänge können – weil es sich nicht um Straftaten handelt – allenfalls zum Zweck einer zeitlich befristeten Dokumentation und/oder zur Vorgangsverwaltung gespeichert werden. Deshalb hat die Speicherung der Daten und die Aufbewahrung der Unterlagen außerhalb der Kriminalaktenhaltung zu erfolgen. Für die Löschung sind besondere Fristen vorzusehen.

Die durch Zuspeicherung unterschiedlicher Deliktsarten entstehende *„Fristenspirale“* wird nicht abgeschafft.

Unsere Stichprobenuntersuchung hat ergeben, dass die *Verlängerung der Prüffrist nicht hinreichend dokumentiert* wird. Nicht selten konnte – auch von den Polizeimitarbeitern – nur vermutet werden, worauf eine Verlängerung auf den festgesetzten Termin für die Prüffrist zurückzuführen ist. Der Polizeipräsident hält die Dokumentierung für ausreichend.

Nur bei der Festsetzung der *Prüffristen bei Fällen von geringer Bedeutung* wurde eine Konsequenz gezogen: Sofern der Wert für die Zuordnung als Bagatelldelikt (Folge: Speicherungsfrist bei Erwachsenen fünf Jahre) maßgeblich ist, wurde die Wertgrenze auf DM 200,00 erhöht. Das bleibt aber immer noch hinter Regelungen in anderen Ländern zurück. In Baden-Württemberg z. B. ist die Wertgrenze DM 500,00 und die Speicherungsfrist in diesen Fällen für Erwachsene nur drei Jahre.

Polizeiliche Beobachtung

> *Auf seinen Antrag auf Auskunft über die zu seiner Person bei der Polizei gespeicherten Daten ist einem Bürger nur eine Teilauskunft erteilt worden. Für weitere gespeicherte Daten wurde ihm die Auskunft unter Hinweis auf § 50 Abs. 2 ASOG verweigert. Die in der Kriminalakte enthaltenen Ergebnisse von polizeilichen Beobachtungen aus den Jahren 1988 und 1989 wurden nicht mitgeteilt.*

Der Akte sind keine relevanten Erkenntnisse aus den Beobachtungen zu entnehmen. Die *Auskunft* wurde dennoch wegen einer prognostizierten Wiederholungsgefahr nicht erteilt. Deshalb sei – frei nach dem Motto „Viele kennen zwar dieses polizeiliche Instrument, wissen aber nicht, dass es gegen sie eingesetzt wird“ – die Kenntnis des Petenten über bereits stattgefundene Beobachtungen nicht zweckdienlich. Darüber hinaus sei die *polizeiliche Beobachtung* vor In-Kraft-Treten des ASOG beendet worden.

Nach unserer Prüfung wurden die Daten im ISVB gelöscht und die dazugehörigen Unterlagen aus der Kriminalakte vernichtet. Der Polizeipräsident bat uns ausdrücklich darum, dem Petenten darüber nichts mitzuteilen, weil er die Geheimhaltung dieser Maßnahme weiterhin für erforderlich hält.

Das Ergebnis kann trotz der Löschung im ISVB und der Vernichtung der dazugehörigen Unterlagen nicht befriedigen, weil der Betroffene so nicht erfährt, was in der Vergangenheit über Jahre hinweg zu seiner Person gespeichert war – und möglicherweise auch anderen Stellen mitgeteilt wurde. Selbst wenn die polizeiliche Beobachtung vor In-Kraft-Treten des ASOG abgeschlossen war, wurden die aus der Maßnahme erlangten Daten noch weiter gespeichert. Die Speicherung der Daten stellt einen Dauertatbestand dar, auf den die Vorschriften des ASOG in der jeweiligen Fassung anzuwenden sind. Auch für diese Altfälle hat damit eine Unterrichtung der Betroffenen nach § 27 Abs. 5 i.V.m. § 25 Abs. 7 ASOG zu erfolgen. Die Auskunft kann nur verweigert werden, wenn eine Abwägung ergibt, dass die schutzwürdigen Belange des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen (§ 50 ASOG). Dies ist hier nicht der Fall.

Vielmehr ist nach Abschluss der Maßnahme die beobachtete Person zu benachrichtigen, sobald das ohne Gefährdung des Zweckes der Maßnahme geschehen kann. Der Gesetzgeber hat hier ausdrücklich auf die Gefährdung des Zweckes der getroffenen Maßnahme Bezug genommen. Prognosen für die Gefährdung künftiger Zwecke spielen in diesem Zusammenhang keine Rolle.

Mitteilung über den Verfahrensausgang

Auf seinen Antrag teilte die Polizei einem Petenten mit, dass er als Tatverdächtiger einer Straftat im ISVB gespeichert ist. Der Petent war darüber irritiert, da er von diesem Tatverdacht freigesprochen wurde.

Nach § 32 Justizmitteilungsgesetz (JuMiG) hat die Staatsanwaltschaft die Polizei über den *Ausgang von Strafverfahren* zu unterrichten. Diese hat die gespeicherten Daten entsprechend zu ändern oder zu löschen, damit kein falsches Bild über die betroffene Person entsteht.

Die Staatsanwaltschaft hat bereits seit 1998 die Möglichkeit der technischen Übertragung der Datensätze geschaffen, die Polizei ist zu einer Entgegennahme der Daten aber nach wie vor nicht in der Lage. Die Senatsverwaltung für Inneres will im ersten Quartal 2000 mit den Programmierarbeiten für die Entgegennahme der Daten per Magnetbandaustausch beginnen. Der Generalstaatsanwalt beim Kammergericht hat für den Fall, dass am 1. April 2000 eine Entgegennahme der Daten

über den Verfahrensausgang bei der Polizei technisch immer noch nicht möglich ist, angekündigt, die erforderlichen Mitteilungen in Papierform an die Polizeibehörde zu übermitteln.

Die Polizei hat schon jetzt erklärt, dass sie keinesfalls in jedem Fall eine Einzelfallüberprüfung nach § 48 ASOG vornehmen wird, wenn die Verfahrensausgänge automatisch in das ISVB eingestellt werden. Lediglich die Einstellungen nach § 170 Abs. 2 StPO, bei denen die Unschuld der Tatverdächtigen bzw. kein Straftatbestand festgestellt wurde, sollen zu Prüfungen führen. In allen anderen Fällen werde die Einzelfallprüfung nur dann durchgeführt, wenn der Betroffene einen Antrag auf Auskunft über die zu seiner Person gespeicherten Daten und/oder auf Löschung stellt.

Unabhängig davon, ob die Mitteilung der Staatsanwaltschaft über den Ausgang des Verfahrens in Papierform oder automatisiert erfolgt, handelt es sich um Informationen, die eine Löschung, Berichtigung oder Ergänzung der gespeicherten Daten erforderlich machen. Nach § 48 Abs. 2 ASOG hat die Daten verarbeitende Stelle die Prüfung durchzuführen, ob die Kenntnis der Daten zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben noch erforderlich ist. Bei dieser klaren Rechtslage kommt es nicht auf Fallzahlen an und wie sie mengenmäßig zu bewältigen sind.

BMo-Office

Mit dem Berliner Modell will der Polizeipräsident in Berlin ein Reformvorhaben umsetzen, welches dem Sicherheitsbedürfnis der Berliner Bevölkerung noch mehr Rechnung tragen soll. Wegen einer Vielzahl öffentlich gewordener Pannen ist das Projekt ins Gerede gekommen. Ein polizeiintern entwickeltes IT-Verfahren und dessen störungsbehafteter Probeeinsatz waren in der Presse und bei den betroffenen Polizeibeamten Hauptzielpunkt der Kritik.

Das Projekt startete vor fünf Jahren unter der Bezeichnung *DiBA-mobil* (Mobile Datenverarbeitung in Berliner Abschnitten)[76]. Folgende Ziele sollten mit diesem Projekt erreicht werden:

- Rationalisierung von Arbeitsvorgängen,
- Beschleunigung der Vorgangsbearbeitung,
- Erhöhung des Qualitätsstandards,
- Vermeidung von Doppelerfassung,
- Verringerung der Druck- und Lagerkosten,
- Verbesserung der Auskunftsmöglichkeiten,
- Übernahme einmal erfasster Angaben in weitere Formulare,

[76] JB 1997, 2.3

- Rationalisierung der Ortsangaben,
- Plausibilitätsprüfung an Ort und Stelle und
- problemlose Fehlerkorrektur/Vorgangsergänzung.

Als die erwähnten technischen Probleme überhand nahmen und die öffentliche Diskussion zu Zweifeln am gesamten Modell führte, wurde das Verfahren im Juli 1998 unter der Bezeichnung DiBA-Formularschrank neu ausgeschrieben.

Das Ergebnis erhielt die Bezeichnung *BMo-Office* (Berliner Modell – Office). Es dient der *formulargestützten Vorgangsbearbeitung* der Landesschutzpolizei. Die bisher in Papierform verwendeten Formulare wurden in ein elektronisches Format übertragen, so dass sie am Rechner ausgefüllt werden können, wobei die Erfassung von personenbezogenen Daten (z. B. von Beschuldigten) in den Erfassungsmasken mit vordefinierten Feldern gesteuert wird. Der Inhalt von Feldern, die in verschiedenen Formularen gebraucht werden (z. B. Adressangaben), kann nach erstmaliger Eingabe immer wieder verwendet werden. Die fertig ausgefüllten Formulare werden ausgedruckt, denn nach wie vor sind die Akten maßgeblich. Deshalb werden alle Vorgänge nach einer bestimmten Frist ohne weitere Prüfung automatisch gelöscht.

BMo-Office wird zunächst nur auf Einzelplatzrechnern in den Abschnitten und Notebooks in den Einsatzfahrzeugen eingesetzt. Eine Netzwerkversion ist für die Zukunft geplant, so dass auch Auskunftsstellen eingerichtet werden können.

Für BMo-Office wird das Betriebssystem MS-Windows NT 4.0-Workstation eingesetzt. Als Dateisystem wird ausschließlich NTFS eingesetzt, welches die „erweiterten“ Sicherheitsfunktionen von Windows NT aktiviert, die den Zugriff auf Dateien und Verzeichnisse über die Zugriffskontrollliste steuern.

Es wurde eine Vielzahl sinnvoller Sicherheitsmaßnahmen getroffen, die ihre Bedeutung vor allem in mobilen Einsatzumgebungen finden, in denen es darauf ankommt, auch in Stresssituationen einfache technische Hilfsmittel zur Verfügung zu haben. Insgesamt ist die Polizei sehr bemüht, das Verfahren auch in datenschutzrechtlicher und in IT-sicherheitstechnischer Hinsicht so pannenfrei wie möglich zu machen. Allerdings gibt es noch weitere Empfehlungen in Bezug auf eine sichere Systemverwaltung, deren Umsetzung die Polizei bisher noch nicht zusagen möchte. So sind wir der Auffassung, dass die Personalnummer nicht zur Authentifizierung verwendet werden darf.

4.2 Ordnungsverwaltung

4.2.1 Die Abschichtungsdebatte

Das *3. Gesetz zur Reform der Berliner Verwaltung* (Verwaltungsreform-Grundsätze-Gesetz, VGG), mit dem weit reichende Veränderungen im Personal-, Haushalts- und Organisationsbereich der Berliner Verwaltung vorgenommen werden, ist seit Ende Mai 1999 in Kraft[77].

Das Gesetz enthält eine *Experimentierklausel,* mit der bis Ende 2001 zeitlich befristet Möglichkeiten zu bürgerorientierten Verfahrenserleichterungen und Zuständigkeitsverlagerungen im Meldewesen erprobt werden können. Die Bürgerämter werden ermächtigt, im Namen des *Landeseinwohneramtes* (LEA) – und umgekehrt die Mitarbeiter des LEA für das jeweilige *Bürgeramt* – nach außen zu handeln. Sie werden insoweit Teil der auftraggebenden Stelle und sind befugt, personenbezogene Daten im Rahmen der für die auftraggebende Stelle geltenden Bestimmungen zu verarbeiten *(Mandat)*[78].

Die Experimentierklausel lässt offen, durch wen und in welchem Umfang an Bürgerämter oder Mitarbeiter des LEA Aufgabenübertragungen erfolgen sollen. Unsere Anregung, eine Verordnungsermächtigung zu schaffen, mit der dann die Einzelheiten – aber auch das Verfahren bei Inkompatibilitäten bei der gleichzeitigen Wahrnehmung von Aufgaben der Leistungs- und der Ordnungsverwaltung geregelt werden könnten, wurde nicht aufgegriffen. Organisatorische Fragen und die Festlegung der Aufgaben, die nunmehr von den Mitarbeitern des Bürgeramtes und der Meldestelle durchgeführt werden, sind vielmehr in einer „Verwaltungsvereinbarung über die Errichtung verzahnter Bürgerämter“ geregelt.

Am 28. Mai 1998 fasste das Abgeordnetenhaus den Beschluss, dass „alle bisher dezentral von den Meldestellen wahrgenommenen Aufgaben des Landeseinwohneramtes (Melde-, Pass-, Ausweiswesen, verschiedene Kraftfahrzeugangelegenheiten u. a.) auf die Bezirke übergehen“ sollen. Daneben soll das Landeseinwohneramt die notwendigen zentralen Aufgaben wahrnehmen und „Kopfstelle für die bezirklichen Meldestellen“ werden[79].

Noch bevor die Experimentierklausel in Kraft trat, wurde von der Senatsinnenverwaltung auftragsgemäß der Entwurf eines Gesetzes zur Neuregelung der *Zuständigkeiten des Landeseinwohneramtes* vorgelegt. Dieser Entwurf, der in der Folgezeit im Abgeordnetenhaus und anderen Gremien heftig diskutiert wurde, enthält Regelungen, die mit der bestehenden Rechts- und Verfassungslage nicht vereinbar sind.

---

77 JB 1998, 4.2.1
78 JB 1997, 4.8.1
79 Abghs.-Drs. 13/2738

Die Probleme ergeben sich daraus, dass die Bezirksämter nach dem Entwurf zwar Melde-, Ausweis- und Passbehörden werden sollen, daneben aber das Landeseinwohneramt zur Führung des Melderegisters zuständig bleiben soll. Das Datenschutzrecht in Bund und Ländern geht davon aus, dass die Daten verarbeitende Stelle personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt. Sie ist damit auch für die Datenverarbeitung verantwortlich. Die Befugnis und Verantwortung für die Verarbeitung der erforderlichen personenbezogenen Daten ist an die gesetzliche Zuweisung der materiellen Aufgabe gebunden. Die *Aufspaltung von materieller Aufgabenzuweisung und Zuständigkeit* für die hierfür erforderliche Verarbeitung personenbezogener Daten ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.

Von diesem Grundsatz gehen die bundesrechtlichen Regelungen (Personalausweisgesetz, Passgesetz, Melderechtsrahmengesetz) aus, die vom Landesgesetzgeber nicht geändert werden können. Danach dürfen nur die Ausweis-, Pass- und Meldebehörde – denen die jeweiligen materiellen Aufgaben und Befugnisse zugewiesen sind – die hierfür erforderlichen Register führen. Diese bundesrechtlichen Regelungen lassen jeweils nur ein Register zu. Ausweislich der Gesetzesmaterialien ist eine zusätzliche *zentrale Registerführung* ausgeschlossen.

Damit gibt es nur zwei Möglichkeiten: Entweder das LEA bleibt Melde-, Pass- und Ausweisbehörde, und die Bezirksämter werden ermächtigt, für das LEA zu handeln, oder aber die Zuständigkeiten werden auf die Bezirksämter abgeschichtet. In diesem Fall können die Bezirke umgekehrt dem LEA einzelne Arbeitsschritte übertragen oder – was im Hinblick auf die Verwaltungsreform konsequent wäre – ein oder mehrere Bezirksämter im Rahmen der Regionalisierung mit der Wahrnehmung beauftragen.

Diese Auffassung wird von der Senatsverwaltung für Inneres nicht geteilt. Sie hat vielmehr den – im Wesentlichen unveränderten – Entwurf in das Mitzeichnungsverfahren gegeben.

4.2.2 Meldewesen, Wahlen, Standesämter

Meldewesen

Der zu lange und immer wieder angekündigte Entwurf für die Novellierung des *Meldegesetzes*[80] wurde trotz einer im Unterausschuss „Datenschutz“ gemachten Zusage auch im Berichtsjahr nicht vorgelegt. Das Abgeordnetenhaus hat nunmehr in seinem Beschluss zum Jahresbericht 1997 die Senatsverwaltung für Inneres aufgefordert, einen Entwurf vorzulegen, der die durch die Änderung des Melderechtsrahmen-

[80] zuletzt JB 1998, 4.2.2

gesetzes vom 11. März 1994 gebotenen Änderungen sowie weitere Vorschläge zur Verbesserung des Datenschutzes berücksichtigt[81].

Inzwischen wird auf Bundesebene bereits ein 2. Gesetz zur Änderung des *Melderechtsrahmengesetzes* beraten.

Dort ist eine Befugnis zur Überprüfung ganzer *Einwohnergruppen* (z. B. mit einer bestimmten Staatsangehörigkeit) vorgesehen, die mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar ist. Bereits konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit der Meldedaten von einzelnen Personen sind danach ausreichend, um die gesamte Gruppe zu kontrollieren. Das kommt einer verdachtslosen und ereignisunabhängigen Kontrolle gleich.

Die *Unterrichtung der Meldebehörde* durch die Empfänger der Meldedaten über dort bekannte Unstimmigkeiten durchbricht gesetzliche Geheimhaltungspflichten wie Berufs- und besondere Amtsgeheimnisse. Dies ist auch im Hinblick auf das öffentliche Interesse an der Richtigkeit des Melderegisters nicht gerechtfertigt. Sofern ein Sozialleistungsträger der Meldebehörde auf diesem Weg Daten übermittelt, handelt es sich um die Offenbarung von Sozialdaten und nicht – wie in der Begründung des Entwurfes ausgeführt – schon um Meldedaten mit der Folge, dass ohnehin eine Offenbarungsbefugnis nach den §§ 67 ff. SGB X erforderlich ist. Auch schließt der Schutzbereich des Steuergeheimnisses nach § 30 AO eine Unterrichtung aus, weil regelmäßig überwiegende schutzwürdige Interessen der Betroffenen vorliegen dürften.

In diesem Gesetzgebungsverfahren versucht die Senatsverwaltung für Inneres neue Regelungen zur *Auskunftssperre*[82] im Rahmenrecht festzuschreiben. Melderegisterauskünfte sollen trotz einer Sperre erteilt und die bisherige unzulässige Praxis[83] legitimiert werden. Wir hätten es begrüßt, wenn die Bundesratsinitiative in die Richtung des Schleswig-Holsteinischen Meldegesetzes gegangen wäre, die Schutzwirkung der Auskunftssperre auch gegenüber den öffentlichen Stellen zu erweitern. Ebenfalls hätte die Novellierung zum Anlass genommen werden können, rahmenrechtlich die Rückmeldung von Auskunftssperren an andere Meldebehörden zu regeln, in deren Einzugsgebiet der Meldepflichtige mit weiteren Wohnungen gemeldet ist.

Statt des erwarteten Gesetzentwurfes zum Landesmeldegesetz hat uns im Frühjahr ein Entwurf zur Änderung der *DVO-MeldeG* erreicht, mit der der Kreis der abfrageberechtigten öffentlichen Stellen um die Finanzbehörden sowie die Gerichte und Staats- und Amtsanwaltschaften erweitert werden sollte.

---

81 Abghs.-Drs. 13/3840, vgl. Anlage 2
82 JB 1996, 4.2.1
83 JB 1996, 4.2.1

Voraussetzung für die Zulässigkeit der Einrichtung eines automatisierten Abrufverfahrens ist, dass diese Form der Datenübermittlung angemessen ist (§ 15 Abs. 1 BlnDSG). Dabei sind die schutzwürdigen Interessen der Betroffenen und die Aufgaben der beteiligten öffentlichen Stellen abzuwägen. Es besteht Einvernehmen mit der Senatsverwaltung für Inneres darüber, dass vor der Einrichtung eines automatisierten Abrufverfahrens im Einzelfall nicht nur der Anlass und der Zweck nachgewiesen werden müssen, sondern auch, ob es sich um eine erhebliche Zahl von Fällen und nicht um seltene Ausnahmen handelt. Im letzteren Fall wäre der Zugang zum Gesamtbestand des Melderegisters unverhältnismäßig. Weiterhin muss die Erforderlichkeit der Datenarten, die zum Abruf bereitgehalten werden sollen, nachgewiesen werden. Dies ist hier nicht der Fall.

Bei dem Entwurf wird auch nicht hinreichend deutlich, ob jeder einzelne Mitarbeiter dieser Stellen den Zugang zum Melderegister erhalten soll oder nur ein oder wenige Terminal(s) zentral aufgestellt werden soll(en), die der gesamten Dienststelle als Auskunftsstelle zur Verfügung stehen. Im letzteren Fall ist nicht einmal eine Erleichterung und somit eine Rechtfertigung für die Einrichtung eines kostenintensiven automatisierten Abrufverfahrens zu erkennen. Es macht keinen Unterschied, ob die Mitarbeiter in der zentral eingerichteten Stelle ihres Amtes oder direkt bei dem LEA nachfragen.

Melderegisterauskünfte durch Wegzugsbehörden

Eine junge Frau wurde von ihrem Ex-Ehemann verfolgt und bedroht. Sie floh vor ihm und zog in ein anderes Bundesland. Damit ihre Adresse nicht bekannt wird, wurde eine Auskunftssperre beim Melderegister eingetragen. Sie war vollkommen verstört, als sie erfuhr, dass ihr Ex-Ehemann ihre neue Adresse bei der Meldestelle für ihre vorherige Wohnung erfahren hatte.

Nach Wegzug eines Einwohners in den Zuständigkeitsbereich einer anderen Meldebehörde und der dortigen Anmeldung erfolgt eine Rückmeldung. Die neue Anschrift ist somit der *Wegzugsbehörde* bekannt und wird auf Anfrage mitgeteilt. Die meisten Länder – so auch Berlin – melden nur die neue Anschrift, nicht aber die Auskunftssperren zurück. Die Betroffenen sollen lediglich darauf hingewiesen werden, dass sie auch bei der Wegzugsbehörde eine solche Sperre beantragen können.

Zur Eintragung einer *Auskunftssperre* muss der Meldepflichtige die mögliche Beeinträchtigung sehr hoher Rechtsgüter glaubhaft darlegen. Seine schutzwürdigen Interessen dürfen durch die Verarbeitung personenbezogener Daten nicht beeinträchtigt werden (§ 6 MRRG). Dies ist aber der Fall, wenn entgegen der Auskunftssperre durch eine andere – örtlich inzwischen unzuständige – Meldebehörde, die davon keine Kenntnis hat, eine Melderegisterauskunft erteilt wird. Eine Mitteilung

der neuen Adresse durch die Wegzugsbehörde ist nur dann hinnehmbar, wenn auch eine Rückmeldepflicht hinsichtlich der Auskunftssperre besteht.

LEA arbeitet immer noch mit DDR-Daten

Seit zwei Jahren steht eine Antwort auf unsere Beanstandung wegen der Verwendung der alten Meldekarteikarten im Ostteil der Stadt aus. Diese enthalten unzulässige Daten (beispielsweise PKZ, Beruf, Hinweise auf den Wehrdienst, Haft sowie Ein- und Ausreisen).

Nach dem Einigungsvertrag sind sämtliche Dateien, die nach den in der DDR an jeden Einwohner vergebenen *Personenkennziffern* (PKZ) geordnet sind, nach anderen Merkmalen umzuordnen. Die PKZ ist in allen Dateien zum frühestmöglichen Zeitpunkt zu löschen. Die über den Katalog des § 2 MeldeG hinausgehenden Daten auf den alten *Meldekarteikarten* werden ohne Rechtsgrundlage – weiter – gespeichert. Seit 1991[84] haben wir gefordert, dass auf den Karteikarten zumindest anlassbezogen die unzulässigen Daten geschwärzt werden.

Bis zur Einrichtung entsprechender EDV-Geräte in den Meldestellen der östlichen Bezirke wurde weiterhin mit den alten Meldekarteikarten gearbeitet. Bezüglich der unzulässig gespeicherten Daten besteht ein Nutzungsverbot, über das die Meldestellen der östlichen Bezirke informiert wurden. Entgegen unserer Forderung schien dem Senat aufgrund der bis spätestens Ende 1993 geplanten Umstellung auf die EDV-Bearbeitung die Unkenntlichmachung der PKZ auf den Meldekarten – z. B. durch Schwärzung – wegen des erheblichen und kostenintensiven Arbeitsaufwandes nicht sinnvoll zu sein[85]. Die Meldebehörde hat darüber hinaus sogar festgelegt, dass die rechtswidrig gespeicherten Daten an Strafverfolgungsbehörden übermittelt werden dürfen. Die Übermittlung unzulässig gespeicherter und rechtswidrig nicht gelöschter Daten verstößt gegen § 25 MeldeG. Danach dürfen nur die nach § 2 MeldeG – zulässigerweise – gespeicherten Daten übermittelt werden.

Auch nach Ablauf von fast zehn Jahren deutscher Einheit sind noch immer nicht alle Meldestellen mit einem Online-Anschluss an das EWW-System ausgestattet, so dass weiterhin mit den Meldekarteikarten gearbeitet werden muss.

Wenn IuK-Technik auf der Straße liegt

Kurz nachdem das Zentrale Fundbüro im Landeseinwohneramt uns nach dem datenschutzgerechten Umgang mit aufgefunden Geräten der Informations- und Kommunikationstechnik gefragt hatte, wandte sich

---

84 JB 1991, 2.2
85 Stellungnahme des Senats zum JB 1991, Abghs.-Drs. 12/1760

eine aufgebrachte Bürgerin an uns. Sie hatte ein Handy gefunden, beim Fundbüro abgegeben und bestand auf der Übereignung des Funktelefons, nachdem der Verlierer sich nicht gemeldet hatte.

Die *Fundbüros* füllen sich inzwischen mit Geräten der Informationstechnik. Vor allem Handys werden immer wieder als Fundsache abgegeben. Möglicherweise werden sie auch nur weggeworfen, weil ein Providervertrag abgelaufen ist und zu einem neuen Vertrag neue Handys kostenlos oder für einen Marginalbetrag ausgehändigt werden. Gelegentlich werden auch andere informationstechnische Systeme, vor allem Laptops, angeliefert. Für das zentrale Fundbüro des *Landeseinwohneramtes* stellte sich die Frage, wie mit solchen Geräten, die möglicherweise schutzwürdige Daten enthalten, datenschutzgerecht umzugehen ist. Die Fragestellung hat verschiedene Aspekte:

Ermittlung des *Finders:* Das Zentrale Fundbüro ist verpflichtet, im zumutbaren Rahmen den Eigentümer zu ermitteln. Bei PCs, Laptops oder Notebooks sind meist keine Schutzmaßnahmen getroffen worden, die Dritte daran hindern, das System in Betrieb zu nehmen. Sofern auf dem System lizenzierte Software installiert ist, dürfte beim Aufruf eines solchen Programms der Lizenzinhaber angezeigt werden. Darüber hinaus könnten Dateiinhalte Rückschlüsse auf den Urheber zulassen, was ebenfalls zum Eigentümer solcher Systeme führen würde. Auch bei Mobiltelefonen kann über die enthaltene Chipkarte der Provider und über ihn der Besitzer ermittelt werden. Sollten PIN-, Passwort- oder Verschlüsselungsschutz die Inbetriebnahme eines Rechners oder Kenntnisnahme von Daten verhindern, so wäre die Ermittlung des Eigentümers auf die beschriebene Weise nicht ohne weiteres möglich. In diesem Falle darf nicht versucht werden, die Schutzmaßnahmen anzugreifen, weil damit die Strafvorschriften des Berliner Datenschutzgesetzes (§ 32 BlnDSG) oder Bundesdatenschutzgesetzes (§ 43 BDSG) berührt sein können.

Weiternutzung der Systeme durch Finder oder *Ersteigerer:* Obwohl gerade die installierte Software den Wert eines IT-Systems ausmachen kann und somit die wirtschaftliche Verwertung für den Finder oder – im Versteigerungsfalle – für das Fundbüro interessanter machen würde, ist die Löschung der Software zwingend geboten, denn weder der Finder noch ein Ersteigerer erlangen Rechte an der Software. Sie würden bei ihrer Nutzung gegen das Software-Urheberrecht verstoßen. Die Lizenz zur Nutzung der Software geht mit dem Verlust des Rechners nicht verloren. Meistens kann der Verlierer bzw. Besitzer die Software, die er in der Regel auf Originaldatenträgern unabhängig vom Rechner aufbewahrt, auf einem Ersatzrechner installieren. Die Nutzung eines gefundenen Mobiltelefons mit der einliegenden SIM-Karte dürfte ohne Kenntnis der PIN nicht möglich sein. Aber selbst dann, wenn es ausnahmsweise gelingt, den PIN-Schutz zu umgehen, wäre die Nutzung unzulässig, denn die Gesprächskosten gehen auch weiterhin zu Lasten des ursprünglichen Besitzers.

4.2.2

Umgang mit schutzbedürftigen Daten: Die *Weitergabe* personenbezogener Daten an Finder oder Ersteigerer verletzt die informationelle Selbstbestimmung der Betroffenen, so dass die Löschung dieser Daten geboten ist. Dritte können gegen den Willen der Betroffenen und des Verlierers keine Rechte an den Daten erwerben.

Daraus ergibt sich, dass für den Fall, dass für einen tragbaren Computer oder einen PC der rechtmäßige Eigentümer nicht festgestellt werden kann, alle Speicher, mit denen der Rechner ausgestattet ist, d. h. insbesondere die Festplatte(n), vollständig und datenschutzgerecht gelöscht werden müssen. Die Löschung hat so zu erfolgen, dass eine Wiederherstellung mit gängigen Programmen nicht möglich ist. Das bedeutet, dass mindestens eine Löschung durch Überschreiben erfolgen muss. Möglicherweise ist es wirtschaftlicher, die Festplatte auszubauen, zu zerstören und ggf. durch eine neue zu ersetzen.

Bei Mobiltelefonen ist die *SIM-Karte* zu entfernen. Es ist möglich, dass das Mobiltelefon dennoch personenbezogene Daten, z. B. für die Kurzwahlfunktion, speichert. Manche Handys bieten es an, auszuwählen, ob solche Daten vertragsabhängig (also auf der SIM-Karte) oder geräteabhängig (im Handy) gespeichert werden. Diese Daten sind vor der Weitergabe des Mobiltelefons ebenfalls zu löschen. Dazu bedarf es der Verwendung einer SIM-Karte, deren PIN dem Fundbüro bekannt ist, denn sonst ist die Löschung dieser Daten nicht möglich.

Standesämter

Immer wieder erreichen uns Anfragen von Familienforschern, die wissen wollen, warum ihnen der Datenschutz den Zugang zu den bei den Standesämtern geführten Personenstandsbüchern verwehrt. Schließlich handelt es sich um Personen, die schon lange – zum Teil mehr als 100 Jahre – verstorben sind.

Die allgemeinen Bestimmungen der Datenschutzgesetze treten zurück, wenn bereichsspezifische Spezialregelungen vorhanden sind. Nach § 61 Personenstandsgesetz (PStG) kann *Einsicht* in die *Personenstandsbücher,* Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden nur von den Behörden im Rahmen ihrer Zuständigkeit und von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Anderen Personen steht dieser Anspruch nur zu, wenn sie ein rechtliches Interesse glaubhaft machen, d. h. die Kenntnis der Personenstandsdaten eines anderen zur Verfolgung von Rechten oder zur Abwehr von Ansprüchen erforderlich ist. Das Landgericht Hamburg hat festgestellt, dass kein rechtliches Interesse vorliegt, wenn die Auskünfte lediglich zu privaten Forschungszwecken benötigt werden[86]. Im Übrigen kann ein

[86] Beschluss v. 28. 7. 1980, Az.: IT 213/80

Inforamtionsrecht auch nicht aus Art. 5 GG hergeleitet werden, weil es sich bei den Personenstandsbüchern nicht um allgemein zugängliche Quellen handelt.

Die Personenstandsbücher sind nicht aus datenschutzrechtlichen Erwägungen für die *Familienforschung* unzugänglich. Aus der Entstehungsgeschichte des § 61 PStG ergibt sich, dass nicht die typischen Gefahren einer elektronischen Datenverarbeitung den Gesetzgeber veranlasst haben, die Nutzung der Personenstandsbücher nur beschränkt zuzulassen. Vielmehr führten die Erfahrungen mit dem Missbrauch, der im Dritten Reich mit den Büchern betrieben wurde, 1957 zum Erlass des § 61 PStG in der noch heute gültigen Fassung. Das Gesetz über die Beurkundung des Personenstandes und die Eheschließung von 1875 sah den unbeschränkten Zugang zu den Personenstandsbüchern vor. Danach war jedem Einsicht zu gewähren und auf Verlangen mussten beglaubigte Auszüge erstellt werden. Die 1937 erlassene neue Fassung des Personenstandsgesetzes bildete die gesetzliche Grundlage für die Ausnutzung der Personenstandsbücher zur Verfolgung religiöser und ethnischer Minderheiten im Dritten Reich.

In der vergangenen Legislaturperiode ist im Bundestag eine Neufassung des § 61 PStG diskutiert worden, wonach zur Einsichtnahme in die Personenstandsbücher ein berechtigtes Interesse genügen sollte[87]. Das ist ein verständiges, durch die Sachlage gerechtfertigtes Interesse, also beispielsweise auch *genealogische Forschung.* Voraussetzung sollte sein, dass seit dem Tod des Betroffenen mindestens 30 Jahre oder seit seiner Geburt mindestens 120 Jahre vergangen sind. Dieser Gesetzentwurf ist allerdings nicht mehr verabschiedet worden. Wir würden es begrüßen, wenn der Senat hier im Interesse der Familienforscher initiativ werden würde.

4.2.3 Ausländische Bürger und Gäste

Bonitätsprüfung bei Gastgebern von Ausländern

Im Jahresbericht 1998[88] haben wir darüber berichtet, dass mit der Senatsverwaltung für Inneres eine Übereinstimmung hinsichtlich einer datenschutzgerechten Verwendung des bundeseinheitlichen Vordrucks für die *Verpflichtungserklärung* nach § 84 Ausländergesetz (AuslG) erzielt werden konnte, mit der sich der *Gastgeber eines ausländischen Besuchers* zur Übernahme gewisser Leistungen verpflichtet. Wie bundesweit üblich wird auch in Berlin auf Eintragungen in den Feldern „Beruf", „Mieter/Eigentümer", „Arbeitgeber" und „Sonstige Angaben zu Wohn-, Einkommens- und Vermögensverhältnissen" verzichtet.

---

87 JB 1996, 4.2.2
88 JB 1998, 4.2.3

4.2.3

Für die Entgegennahme der Verpflichtungserklärung sind in Berlin die Meldestellen zuständig. Sie informieren die potenziellen Gastgeber schriftlich über das Verfahren sowie die Konsequenzen einer abgegebenen Erklärung. Die Betroffenen werden gebeten, die erforderlichen Angaben auf einem gesonderten Vordruck – der bundeseinheitliche Vordruck wird zur Vermeidung von Missbrauch dem Antragsteller nicht ausgehändigt – zu machen. Auf diesem Vordruck werden die Felder, die Detailangaben zu Wohn-, Einkommens- und Vermögensverhältnissen betreffen, durch die Dienstkraft der Meldestelle vor Aushändigung gestrichen. Die vom Antragsteller gemachten Angaben werden sodann von der Dienstkraft der Meldestelle in den bundeseinheitlichen Vordruck übertragen. Dieser wird mit dem Dienststempel des Landeseinwohneramtes versehen und dem Auswärtigem Amt bzw. der zuständigen deutschen Auslandsvertretung des Landes, aus dem der Gast einreisen will, übersandt[89].

Mehrfach erhielten wir daraufhin Beschwerden von Berlinern, die ihre ausländischen Freunde oder Familienangehörige einladen wollten. Ihre in Berlin ausgefüllten Vordrucke zur Verpflichtungserklärung wurden von den Auslandsvertretungen als unzureichend zurückgewiesen. Es wurden weitere Nachweise zur Einkommenssituation vom Antragsteller verlangt. Diese waren zu Recht verärgert. Das Verfahren wurde durch diese Maßnahme unzumutbar verlängert, zumal die Unterlagen von den Antragstellern bereits in Berlin bei den zuständigen Meldestellen vorgelegen haben.

Nach Mitteilung des Bundesbeauftragten für den Datenschutz – der die Angelegenheit beim Auswärtigen Amt bzw. den zuständigen Auslandsvertretungen überprüft hat – handelte es sich um ein spezifisches Berliner Problem. In den anderen Bundesländern wird, anhand der vom Antragsteller eingereichten Unterlagen, eine Bonitätsprüfung durchgeführt und das Ergebnis pauschal in dem Vordruck bestätigt, ohne dass Einzeleintragungen in den Feldern „Wohn-, Einkommens- und Vermögensverhältnisse“ vorgenommen werden. In Berlin dagegen wird die Bonität der Gastgeber von den Meldestellen nicht geprüft und/oder nicht auf der Verpflichtungserklärung nach § 84 AuslG bescheinigt. Dies geschieht nicht etwa aus Gründen des Datenschutzes, sondern allein wegen fehlender personeller und sachlicher Ressourcen in den Antrag bearbeitenden Stellen.

Damit wird die bundeseinheitliche und im Konsens erarbeitete datenschutzgerechte Verfahrensweise, keine Einzelangaben über die finanzielle Leistungsfähigkeit der Gastgeber in die Verpflichtungserklärung aufzunehmen, in Berlin ins Abseits gestellt. Die Verfahrensweise der Berliner Ausländerbehörde provoziert Nachfragen der Auslandsvertretung zur Bonität der Gastgeber bzw. nimmt diese – auf Kosten des Datenschutzes – in Kauf.

---

[89] Kleine Anfrage Nr. 13/5088; LPD 160/99 v. 19. 8. 1999, S. A 7

Die Prüfung und Bescheinigung der Bonität des Gastgebers durch die Ausländerbehörde (ohne Aufnahme von Einzelangaben zur finanziellen Leistungsfähigkeit des Gastgebers in der Verpflichtungserklärung) ist in jedem Fall die wesentlich datenschutzfreundlichere Lösung gegenüber einer Bonitätsprüfung durch die Auslandsvertretungen.

Das Auswärtige Amt hat mit Runderlass vom 2. September 1999 sämtliche deutsche Auslandsvertretungen gebeten, in Zukunft bei Visumsverfahren für einen Kurzaufenthalt von bis zu drei Monaten in der Regel auf die Vorlage von weiteren Unterlagen zu verzichten.

Ausschreibung zur Einreiseverweigerung im Schengener Informationssystem (SIS)

Die in Frankreich für die Kontrolle des Bestandes des Schengener Informationssystems (SIS) zuständige Datenschutzbehörde, die Commission Nationale de l'Information et des Libertés (CNIL), hatte den Bundesbeauftragten für den Datenschutz über das Auskunftsersuchen eines ausländischen Staatsbürgers informiert. Die Nachfrage beim Bundeskriminalamt (BKA) ergab, dass der Betroffene auf Veranlassung des Landeseinwohneramtes Berlin zur Einreiseverweigerung nach Artikel 96 Schengener Durchführungsübereinkommen (SDÜ) im SIS ausgeschrieben worden war. Wir wurden gebeten, die Rechtmäßigkeit der Ausschreibung in diesem Einzelfall zu überprüfen.

Anhaltspunkte für die Beurteilung der Rechtmäßigkeit einer Ausschreibung zur Einreiseverweigerung nach Artikel 96 SDÜ durch die jeweiligen Ausländerbehörden bieten die Allgemeinen Anwendungshinweise zum *Schengener Durchführungsübereinkommen* (AAH-SDÜ) vom 28. Januar 1998. Darin ist detailliert dargelegt, unter welchen ausländerrechtlichen Voraussetzungen Ausschreibungen im SIS nach Artikel 96 SDÜ zulässig und welche Ausschreibungsfristen zu beachten sind.

Bei unserer Prüfung konnten wir keinen Hinweis auf eine Ausschreibung des Betroffenen nach Artikel 96 SDÜ feststellen. Das *Landeseinwohneramt* Berlin hatte mit einem Schreiben vom Dezember 1994 an den Polizeipräsidenten in Berlin lediglich die Ausschreibung des Betroffenen zur Fahndung im INPOL-System beantragt. Zur Erläuterung teilte uns die Ausländerbehörde dazu Folgendes mit: Im Hinblick auf das zum 26. März 1995 vorgesehene In-Kraft-Treten des SDÜ und der Aufnahme des Wirkbetriebes des SIS wurden die zwischen dem 1. Januar 1994 und 27. März 1995 im INPOL erfassten Fälle (ca. 131 000) retrograd in den SIS-Datenbestand übernommen, ohne dass eine Einzelfallprüfung vorgenommen wurde. Erst im Dezember 1997/Januar 1998 wurden vom BKA Überprüfungen der Speicherfristen durchgeführt. Diese Überprüfungen führten im Regelfall zu einer einmaligen automatischen dreijährigen SIS-Restlaufzeit. Erfolgt zwischenzeitlich

keine Reaktion der Ausländerbehörde, werden die Ausschreibungen nach Ablauf dieser Frist automatisch vom BKA – somit spätestens mit Ablauf des Januar 2001 – aus dem SIS-Bestand gelöscht.

Angesichts der Vielzahl der Fälle ist eine nachträgliche Prüfung, ob die ausländerrechtlichen Voraussetzungen für eine Ausschreibung zur Einreiseverweigerung nach Artikel 96 SDÜ gegeben sind, nicht durchführbar. Diese Prüfung hat jedoch anlassbezogen (z. B. wie im vorliegenden Fall bei einem Antrag auf Auskunft bzw. Löschung) zu erfolgen. Das Ergebnis ist in der zur Person des Betroffenen geführten Akte nachvollziehbar zu dokumentieren.

4.2.4 Verkehr

Arbeitsanweisung für die Führerscheinstelle

Seit langem haben wir – zuletzt mit massiver Unterstützung des Unterausschusses „Datenschutz" des Ausschusses für Inneres, Sicherheit und Ordnung – darauf gedrängt, dass für die Mitarbeiter der Führerscheinstelle im Landeseinwohneramt Berlin eine Arbeitsanweisung erlassen wird, mit der den Anforderungen der seit 1. Januar 1999 geltenden neuen straßenverkehrsrechtlichen Bestimmungen über Vernichtungsfristen für bestimmte Unterlagen in den Führerscheinakten Rechnung getragen werden kann[89a] . Diese Arbeitsanweisung liegt nunmehr vor.

Danach sind Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse grundsätzlich nach spätestens 10 Jahren zu vernichten (§ 2 Abs. 9 Straßenverkehrsgesetz (StVG)). Das gesetzliche Verwertungsverbot nach § 52 Abs. 2 Bundeszentralregistergesetz ist zu beachten, das bestimmt, dass die einer Verurteilung zugrunde liegende Tat nach Tilgung im Verkehrszentralregister dem Betroffenen im Verfahren über die Erteilung oder Entziehung einer Fahrerlaubnis nicht mehr vorgehalten werden darf. Unter Berücksichtigung dieser neuen Rechtslage sieht die Arbeitsanweisung vor, dass die Führerscheinakte anlassbezogen derart zu bereinigen ist, dass zunächst grundsätzlich alle Unterlagen, die älter als 10 Jahre sind, zu entfernen sind. Die übrigen Unterlagen werden vernichtet, wenn auch die entsprechenden Eintragungen im Verkehrszentralregister gelöscht sind. Wir meinen, dass diese Verfahrensweise einen gangbaren Weg darstellt, um die Umsetzung der neuen Bestimmungen über Vernichtungsfristen durch die einzelnen Mitarbeiter in der Führerscheinstelle zu gewährleisten. Anhand konkreter Einzelfälle wird sich zeigen, ob die Bestimmungen den datenschutzrechtlich relevanten Problemen in ausreichender Weise Rechnung tragen. In dem folgenden Fall hat sich dies jedenfalls bewahrheitet.

---

89 a zuletzt JB 1998, 4.2.4; JB 1997, 4.2.3

Ein Bürger bat uns um Überprüfung der in der Führerscheinstelle beim Landeseinwohneramt Berlin geführten Fahrerlaubnisakte, die seiner Ansicht nach nicht mehr aufzubewahrende Unterlagen enthalte. Da die unbereinigte Akte an eine Gutachterstelle weitergegeben worden war, hat der Bürger Strafanzeige wegen rechtswidriger Datenübermittlung erstattet.

Die Akte enthielt Unterlagen im Zusammenhang mit einem Strafbefehl aus dem Jahre 1983 sowie Unterlagen, die ein abgeschlossenes Neuerteilungsverfahren aus dem Jahre 1984 betrafen, also Vorgänge, die etwa 15 Jahre zurücklagen. Darüber hinaus gab es Unterlagen, die im Zusammenhang mit der Einrichtung und Aufhebung einer Gebrechlichkeitspflegschaft standen und die in den Jahren 1986 und 1987 der Prüfung dienten, ob die Einleitung eines Fahrerlaubnis-Entziehungsverfahrens erforderlich ist. Da die Straftat im Verkehrszentralregister inzwischen getilgt war und die im Zusammenhang mit dem (später eingestellten) Entziehungsverfahren eingeholten Unterlagen über den Gesundheitszustand des Betroffenen älter als 10 Jahre waren, hat die Führerscheinstelle zugesagt, die Akte nach den Vorgaben ihrer Arbeitsanweisung zu bereinigen und die Unterlagen zu vernichten, sobald das anhängige Strafverfahren beendet ist.

Halterauskunft zu Recht verweigert

Die Senatsverwaltung für Bauen, Wohnen und Verkehr und die BEHALA wollten wissen, ob die Kfz-Zulassungsstelle im Landeseinwohneramt Berlin der BEHALA aus dem örtlichen Fahrzeugregister Auskünfte über Halter von Fahrzeugen in den Fällen erteilen darf, in denen sich der Fahrzeugführer nach dem Abladen von Bauschutt vom Gelände der BEHALA entfernt hat, ohne zuvor das fällige Entgelt zu entrichten. Die Senatsverwaltung und die Kfz-Zulassungsstelle verneinten diese Frage.

Auch wir halten die Erteilung von Halterauskünften in diesen Fällen für unzulässig, weil die Voraussetzungen der hierfür maßgeblichen Bestimmungen der §§ 35, 39 StVG nicht vorliegen. § 39 Abs. 1 erfordert die Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr. Der Anspruch auf Entrichtung des Entgeltes für das Abladen von Bauschutt ist jedoch nicht verkehrsbezogen, so dass die begehrte Halterauskunft nicht in Frage kam, zumal Halter und Fahrer des Kfz in den in Rede stehenden Fällen nicht identisch zu sein brauchen und der wahre Schuldner (nämlich der Fahrer) anhand der Halterauskunft ohnehin nicht zweifelsfrei ermittelbar wäre. Zur Vermeidung von Wiederholungsfällen konnten wir der BEHALA aber empfehlen, künftig die Personalien des Zahlungspflichtigen aufzunehmen, d.h. desjenigen, der den Bauschutt – mit eigenem oder fremdem, ggf. gemietetem Kfz – anfährt. Diese Datenverarbeitung ist zulässig nach § 6 Abs. 1 Satz 1 Nr. 2 BlnDSG und der aufgrund des § 118

Abs. 2 Landeshaushaltsordnung (LHO) ergangenen „Verordnung über die Verarbeitung personenbezogener Daten des Haushaltswesens". Nach deren § 2 können im Zusammenhang mit der Erhebung von Einnahmen, zu denen auch die durch die BEHALA als rechtsfähige Anstalt des öffentlichen Rechts zu erhebenden Entgelte gehören, bestimmte Daten eines Zahlungspflichtigen wie Name, Vorname, Geburtsdatum, Anschrift verarbeitet werden. Zum Nachweis seiner Angaben kann nach § 18 Abs. 1 Passgesetz bzw. § 4 Abs. 1 Personalausweisgesetz die Vorlage eines Ausweises verlangt werden, wobei die Erhebung weiterer im Ausweis enthaltener Angaben genauso unzulässig wäre wie das Kopieren des gesamten Ausweises.

Örtliches Kraftfahrsachverständigenregister mit EDV-Technik

Im Rahmen einer länderübergreifenden Arbeitsgruppe wird ein einheitliches EDV-Programm erstellt, mit dem die in den Ländern geführten örtlichen Kraftfahrsachverständigenregister geführt werden sollen. Während die Erstellung des Programms einer amtlich anerkannten Überwachungsorganisation übertragen wurde, hat Berlin zugesagt, die behördlichen Anforderungen einzubringen. Wir haben das Datenverarbeitungsprogramm anhand der Datenverarbeitungsbefugnisse des seit dem 1. Januar 1999 neu gefassten Kraftfahrsachverständigengesetzes – KfSachvG – überprüft und empfohlen, ein „Datenschutz-, Datensicherungs- und Datenlöschungskonzept" zu erstellen. Die Senatsverwaltung ist dieser Empfehlung gefolgt. Wir haben verschiedene Anregungen zur Ergänzung der Arbeitsanweisung gegeben. So waren Klarstellungen zum Umfang der zu speichernden Daten erforderlich, ebenso zu der entsprechenden Geltung der Löschfristen des § 30 KfSachvG für die in den Akten befindlichen Daten sowie dazu, welche für die Anerkennung bedeutsamen „nachteiligen Tatsachen" im Sinne des § 13 Abs. 3 KfSachvG gespeichert werden dürfen. Die in den Datensatzbeschreibungen vorgesehenen Memo-Felder, deren Inhalt nicht genau bestimmt, sondern z. B. nur als „Bemerkungen der Behörde" beschrieben worden ist, können hinsichtlich ihrer datenschutzrechtlichen Zulässigkeit nicht überprüft werden. Deshalb bedarf es organisatorischer Regelungen z. B. in der Arbeitsanweisung, die eine Aussage zum zulässigen Inhalt treffen. Die Verkehrsverwaltung hat zugesagt, unsere Empfehlungen zu berücksichtigen.

4.3 Justiz und Finanzen

4.3.1 Justiz

Gesetzgebung

Auch die neue Bundesregierung hat einen Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – *Strafverfahrensänderungsgesetz* 1999 (StVÄG 1999)[90] – vorgelegt. Grundlage für diesen Entwurf war der StVÄG-Entwurf von 1996. Allerdings ist der neue Entwurf in einigen wesentlichen Punkten in datenschutzrechtlicher Hinsicht ein Rückschritt:

So sind beispielsweise die *Löschungsfristen* in § 490 Abs. 4 des Entwurfs zur Änderung der StPO (StPO-E) gegenüber dem Entwurf des StVÄG 1996 wesentlich verlängert worden. Die Löschungsfrist für Daten von bei der Tatzeit noch nicht strafmündigen Kindern ist von einem auf zwei Jahre heraufgesetzt worden, die Löschungsfrist für Daten von Jugendlichen von vier auf fünf Jahre und die Frist für Daten von zur Tatzeit über 18-Jährigen von acht auf zehn Jahre. Wir haben erhebliche Zweifel an der Verhältnismäßigkeit der im Entwurf der Bundesregierung noch einmal heraufgesetzten Löschungsfristen. Sie sind undifferenziert und berücksichtigen nicht die unterschiedlichen Anlässe der Speicherung, d. h. die Schwere des Tatvorwurfes.

Auch die Regelung einer *Observation* von mehr als 24 Stunden in § 163 f StPO-E sieht nunmehr – im Gegensatz zum Vorentwurf – den Verzicht auf einen Richtervorbehalt vor. Diese Maßnahme soll nun durch die Staatsanwaltschaft angeordnet werden können. Wir halten einen Richtervorbehalt, wie er auch bei Telefonüberwachungsmaßnahmen gilt, wegen des schwerwiegenden Eingriffes, der mit dieser verdeckten Maßnahme verbunden ist, für die Anordnung für erforderlich.

Auch bei dem neuen StVÄG-Entwurf vermissen wir einen Anspruch des Beschuldigten, der sich selbst verteidigt (unter den in § 147 Abs. 7 StPO-E genannten Einschränkungen), *Akteneinsicht* statt lediglich Auskunft und Abschriften zu erhalten. Die in § 147 Abs. 7 StPO-E jetzt vorgesehene Ermessensregelung dürfte nicht mit dem Urteil des Europäischen Gerichtshofs für Menschenrechte vom 17. Februar 1997[91] zu vereinbaren sein, wonach die Weigerung der Staatsanwaltschaft, dem Beschuldigten bei seiner Verteidigung in eigener Person Akteneinsicht zu gewähren und Kopien aus den Akten zu überlassen, Art. 6 Abs. 3 und 1 Europäische Menschenrechtskonvention verletzt und die Verweigerung der Akteneinsicht den Staat schadensersatzpflichtig macht.

---

90 BR-Drs. 65/99, BT-Drs. 14/1484
91 NStZ 1998, S. 429 f.

4.3.1

Am 2. Juni 1999 hat der Bundestag mit Zustimmung des Bundesrates das Gesetz zur Änderung des *DNA-Identitätsfeststellungsgesetzes* (DNA-IFG) beschlossen[92]. Er hat darin eine rechtliche Grundlage für Datenerhebungen durch die Staatsanwaltschaft und eine korrespondierende Übermittlungsbefugnis des Bundeszentralregisters für die Prüfung der Aufnahme so genannter Alt-Fälle, d. h. bereits Verurteilter, in die DNA-Analyse-Datei geschaffen. Bisher hatte es hierfür keine ausreichende Rechtsgrundlage gegeben.

Außerdem ist im DNA-IFG eine gesetzliche Grundlage für die Speicherung von DNA-Analysen, die im Ermittlungsverfahren zum Zweck des Tatnachweises durchgeführt worden sind, geschaffen worden, wenn die Voraussetzungen des § 81 e StPO vorliegen. Wir verstehen den Gesetzestext des neu eingefügten § 2 Abs. 2 DNA-IFG so, dass eine Speicherung der DNA-Analysen aus Ermittlungsverfahren nur aufgrund einer richterlichen Anordnung nach § 91 f StPO zulässig ist, da es hierzu einer gesonderten richterlichen Prognose bedarf, dass im Einzelfall eine besondere Wiederholungsgefahr hinsichtlich eines im Straftatenkatalog des § 2 e Abs. 4 DNA-IFG aufgeführten Deliktes von erheblicher Bedeutung besteht[93].

Der Bundestag hat am 3. Dezember 1999 den *Täter-Opfer-Ausgleich* in der Strafprozessordnung verankert. Das Parlament verabschiedete einen Gesetzentwurf der Bundesregierung in geänderter Fassung. § 155 b StPO regelt nunmehr die Datenverarbeitung bei der Durchführung des Täter-Opfer-Ausgleiches.

Die zentrale Frage besteht darin, ob bzw. unter welchen Voraussetzungen Opferdaten ohne oder auch gegen den Willen des Betroffenen an privatrechtlich organisierte Schlichtungsstellen übermittelt werden dürfen. Die Gesetzesänderung sieht vor, dass eine Datenübermittlung an die Schlichtungsstellen nur bei einem ausdrücklich geäußerten, entgegenstehenden Willen des Opfers unterbleibt. Der Forderung der Datenschutzbeauftragten des Bundes und der Länder, für diese Datenweitergabe eine unzweifelhafte Einwilligung der Opfer vorzusehen[94], wurde nicht gefolgt.

Zu begrüßen ist, dass in dem Entwurf eines Gesetzes zur Regelung des Vollzuges der *Untersuchungshaft* nunmehr auch für diesen Bereich der Justiz Bestimmungen zu den dort erforderlichen Eingriffen in die informationelle Selbstbestimmung vorgesehen sind, insbesondere zur

---

92 BGBl. I 1999, S. 1242; vgl. auch JB 1998, 4.3.1

93 vgl. auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen", Anlagenband „Dokumente zum Datenschutz 1999", Teil A III

94 Entschließung zu „Täter-Opfer-Ausgleich und Datenschutz", Anlagenband „Dokumente zum Datenschutz 1999", Teil A III

Überwachung der Gefangenen und zur Übermittlung personenbezogener Daten an dritte Stellen. Allerdings hat der Bundesrat in seiner Stellungnahme deutliche Verschlechterungen gegenüber dem Entwurf der Bundesregierung vorgeschlagen[95].

Nach wie vor unbefriedigend sind die Regelungen über die Aufbewahrung der *Justizakten*. Die Konferenz der Datenschutzbeauftragten hat unter Hinweis auf entsprechende obergerichtliche Urteile in einer Entschließung gefordert, dass unverzüglich mit der gesetzgeberischen Arbeit begonnen werden muss. Dies gelte insbesondere auch für Akten der *Zivilgerichte* und der *Freiwilligen Gerichtsbarkeit*[96].

Parlamentarische Kontrolle von Lauschangriffen

Der Gesetzgeber hat bei der Einführung des *Großen Lauschangriffes* im Grundgesetz eine jährliche Berichtspflicht gegenüber dem Parlament vorgeschrieben (Art. 13 Abs. 6 GG). Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichtes die parlamentarische Kontrolle aus. Die Länder haben eine gleichwertige Kontrolle zu gewährleisten.

Für den präventiven Lauschangriff der Polizei wurde im ASOG eine *Berichtspflicht* gegenüber dem Abgeordnetenhaus vorgeschrieben[97]. Für den Lauschangriff zu Strafverfolgungszwecken lehnt die Senatsverwaltung für Justiz eine gesetzliche Regelung, die die parlamentarische Kontrolle der Maßnahmen auf Landesebene absichert, jedoch ab. Sie hält eine Regelung im Rahmen der Geschäftsordnung des Abgeordnetenhauses für ausreichend, da Art. 13 Abs. 6 Satz 1 GG für repressive Maßnahmen eine abschließende Regelung darstelle und damit eine Berichtspflicht der Landesregierung gegenüber dem Landesparlament nicht bestehe.

Die Verantwortung der Exekutivbehörden der Länder besteht nach Art. 28 Abs. 1 Satz 1 i.V.m. Art. 20 GG gegenüber dem Landesparlament und ist Ausdruck der allgemeinen politischen Kontrollfunktion des Parlamentes. Allein die Tatsache, dass nach Art. 13 Abs. 6 Satz 1 GG und § 100 e Abs. 2 StPO gegenüber dem Deutschen Bundestag jährlich ein Bericht zu erstatten ist, der auch die Maßnahmen der Länderbehörden umfasst, ändert nichts an dieser Verantwortlichkeit der Exekutive gegenüber dem Landesparlament. Die Berichtspflicht der Landesjustizverwaltungen soll lediglich gewährleisten, dass der Deutsche Bundestag als Gesetzgeber in diesem Bereich einen Gesamtüberblick

---

95 vgl. hierzu auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Angemessener Datenschutz auch für Untersuchungsgefangene", Anlagenband „Dokumente zum Datenschutz 1999", Teil A II

96 Entschließung zu „Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften", Anlagenband „Dokumente zum Datenschutz 1999", Teil A III

97 vgl. 4.1.1

über alle durchgeführten Maßnahmen erhält. Art. 13 Abs. 6 Satz 3 GG, der eine gleichwertige parlamentarische Kontrolle der Länder vorschreibt, bleibt hiervon unberührt.

Eine sinnvolle Kontrolle auf Landesebene ist aber nur dann möglich, wenn der Senat über alle Maßnahmen berichtet, die von der Berliner Polizei und der Staatsanwaltschaft veranlasst wurden – unabhängig davon, ob die jeweilige Maßnahme auf Bundes- oder auf Landesrecht gestützt worden ist. So hat Bayern eine Berichtspflicht der Staatsregierung gegenüber dem Landtag sowohl bei präventiven als auch repressiven Maßnahmen in einem Gesetz zur Anpassung des bayerischen Landesrechtes an Art. 13 GG geregelt. Offensichtlich sieht auch die bayerische Landesregierung eine wirksame Kontrolle nur in einer umfassenden Berichtspflicht der Landesregierung sowohl über präventiv-polizeiliche als auch repressive Lauschangriffe gegenüber dem Landtag[98].

Das Staatsanwaltschaftliche Auskunftssystem AStA

Eine Bürgerin beschwerte sich darüber, dass ihr in einer Berufungsverhandlung vor dem Landgericht von dem Sitzungsvertreter der Staatsanwaltschaft ein Verfahren entgegengehalten wurde, das bereits 1992 eingestellt worden war.

Folgendes war geschehen: 1992 war ein gegen die Petentin durchgeführtes Ermittlungsverfahren von der Staatsanwaltschaft eingestellt worden. Nach den Aufbewahrungsbestimmungen für die Justiz hätten die im staatsanwaltschaftlichen Verfahren AStA gespeicherten Daten nach fünf Jahren gelöscht und die Akten vernichtet werden müssen. Nach eigenen Aussagen der Staatsanwaltschaft war die Aufbewahrungsfrist Ende 1997 abgelaufen. Die *Löschung* im AStA erfolgt aus technischen Gründen jedoch nur zweimal jährlich. Als der AStA-Ausdruck für den zuständigen Staatsanwalt im Februar 1998 erstellt wurde, hätte das Verfahren im AStA eigentlich schon gelöscht sein müssen, was wegen der erst Mitte des Jahres erfolgenden Aktion jedoch nicht der Fall war. Dem Sitzungsvertreter der Staatsanwaltschaft war dies im Berufungstermin im März 1999 nicht weiter aufgefallen, so dass er das eingestellte Verfahren in der Berufungsverhandlung noch einmal angesprochen hat.

Es herrscht Einigkeit zwischen der Staatsanwaltschaft und uns darüber, dass die Verwendung der Daten des AStA-Auszuges, die zum Zeitpunkt des Sitzungstermines bereits hätten gelöscht sein müssen, unzulässig war. Das Hauptproblem dieses Falles liegt jedoch in der

[98] vgl. auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern“, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A II

nicht fristgerechten Löschung der Verfahrensdaten nach Ablauf der Aufbewahrungsfrist. Eine nur zweimal jährlich erfolgende Löschung nach Fristablauf – nämlich jeweils Mitte und Ende des Jahres – verlängert die fünfjährige Aufbewahrungsfrist immerhin um bis zu einem Fünftel. Der vorliegende Fall zeigt deutlich, dass die bisherige Argumentation der Staatsanwaltschaft, dass es sich bei dem AStA schließlich „nur" um ein internes Vorgangsverwaltungssystem handele, fehlgeht. Im vorliegenden Fall wäre das abgeschlossene Verfahren bei einer fristgerechten Löschung im Februar 1998 nicht mehr auf dem AStA-Ausdruck für den Staatsanwalt erschienen. Darüber hinaus hat der Sitzungsvertreter der Staatsanwaltschaft selbstverständlich auch die Pflicht, bei der Verwendung von AStA-Auszügen zu prüfen, ob die Daten noch genutzt werden dürfen.

Seit vielen Jahren diskutieren wir mit der Staatsanwaltschaft und der Senatsverwaltung für Justiz darüber, wann eine Löschung von Daten im AStA zu erfolgen hat, wenn bei mehreren Beschuldigten das Verfahren gegen einen Beschuldigten abgeschlossen und gegen die anderen weitergeführt wird. Wir vertreten die Auffassung, dass nach Abschluss des Verfahrens gegen einen Beschuldigten für diesen auch die gesetzliche Aufbewahrungsfrist zu laufen beginnt.

Die Senatsverwaltung für Justiz hat uns hierzu jetzt mitgeteilt, dass unsere Auffassung geteilt werde und bei anstehender Neukonzeptionierung des automatisierten Registersystems AStA auch berücksichtigt werden soll.

Aufgrund von Pressemitteilungen stellte sich die Frage, ob gegen Mitarbeiter der Polizei geführte Ermittlungsverfahren, wie alle anderen Ermittlungsverfahren auch, im AStA der Staatsanwaltschaft gespeichert werden.

Tatsächlich sind in der Vergangenheit bei Ermittlungsverfahren gegen *Mitarbeiter der Polizei* deren Daten nicht namentlich im AStA gespeichert worden; stattdessen sei der Eintrag „Bediensteter der Polizei" erfolgt. Nach § 4 der Aktenordnung von Berlin i. V. m. ihrer Ausfüllanleitung für das Js-Register sind nach Auskunft der Staatsanwaltschaft zwingend entweder die Personalien der beschuldigten natürlichen Personen oder aber – falls die Personalien nicht oder noch nicht bekannt sind – nur der Anzeigende in das Register einzutragen. Hiermit steht die bisherige Verfahrensweise nicht im Einklang. Der Generalstaatsanwalt der Staatsanwaltschaft I bei dem Landgericht Berlin hat daher angekündigt, dass er anordnen werde, entsprechend § 47 Aktenordnung in allen Fällen, in denen sich eine Anzeige gegen eine bestimmte Person richtet oder eine solche Person bekannt wird, diese als Beschuldigten einzutragen und den Aktendeckel entsprechend zu

beschriften. In allen anderen Fällen ist der Beschuldigte als „Unbekannt“ zu bezeichnen, und es ist allein der Anzeigende/Geschädigte in das Register einzutragen.

Das „Abhör“-Urteil des Bundesverfassungsgerichtes

Das „Abhör“-Urteil des Bundesverfassungsgerichtes[99] hat auch Auswirkungen auf die Verarbeitung personenbezogener Daten bei der Staatsanwaltschaft, die aus Eingriffen in das Fernmeldegeheimnis stammen. Das Bundesverfassungsgericht hat die Sicherung der Zweckbindung für diese Daten besonders hervorgehoben und als Verfahrensvorkehrung ihre *Kennzeichnung* gefordert. Die Staatsanwaltschaft hat somit diese Daten – unabhängig davon, ob sie sie selbst erhoben oder von anderen Stellen empfangen hat – zu kennzeichnen. Diese Anforderung muss auch Konsequenzen haben für die Verwendung anderer Daten, die einer besonderen Zweckbindung unterliegen.

Datenschutz im Strafvollzug

Auch im Jahr 1999 haben wir unsere Gespräche mit der Justizvollzugsanstalt Tegel und der Senatsverwaltung für Justiz zur Abarbeitung der bei unserer 1995 durchgeführten Querschnittsprüfung festgestellten datenschutzrechtlichen Probleme fortgesetzt[100]. Es wurden abschließend Probleme bei der Datenverarbeitung in den *Arztgeschäftsstellen* der Teilanstalten der Justizvollzugsanstalt Tegel erörtert. Wir haben uns darauf geeinigt, dass Laboruntersuchungen zur Festellung einer *HIV-Infektion* in Zukunft anonymisiert an das Untersuchungslabor übermittelt werden. Bisher wurden dem Labor die Proben mit dem Namen des betroffenen Strafgefangenen zugesandt. Auch die Weitergabe von Daten über HIV-Infektionen bei der Übermittlung von Patientendaten an weiter- bzw. nachbehandelnde Ärzte innerhalb der JVA haben wir mit den Mitarbeitern der Senatsverwaltung für Justiz und des Strafvollzuges erörtert. Es bestand Einigkeit darüber, dass vor jeder Weitergabe einer Patientenakte die Erforderlichkeit der Daten für den Arzt, an den die Akte übermittelt wird, zu prüfen ist. Problematisch ist jedoch derzeit die Herausnahme einzelner Seiten mit nicht erforderlichen Daten aus der Patientenakte. Es wird angestrebt, die Patientenakten in Zukunft durch eine getrennte Heftung übersichtlicher zu gestalten, so dass es möglich wird, die ärztlichen Unterlagen zu einer HIV-Infektion getrennt zu heften und in Zukunft vor einer Weitergabe der Patientenakte herausnehmen zu können. Eine sofortige Änderung des Verfahrens konnten wir leider nicht erreichen. Die Markierung von Patienten-

---

99 Im Einzelnen vgl. 1.1
100 JB 1995, 3.5; JB 1997, 4.3.1; JB 1998, 4.3.1

akten HIV-infizierter Gefangener mit einem „Hängereiter“ mit rotem Punkt im Aktenschrank ist zu statistischen Zwecken nicht erforderlich. Im Gegensatz zu den Mitarbeitern der Senatsverwaltung für Justiz und des Strafvollzuges sehen wir es als problematisch an, dass bei jeder Aktenentnahme oder jedem Weghängen einer Akte und ohne dass dies erforderlich ist, eine Information über HIV-Infektionen in der jeweiligen Arztgeschäftsstelle möglich ist. Wir werden zur Lösung dieses Problems gemeinsam nach Alternativen suchen, Statistiken über HIV-Infektionen in datenschutzgerechter Weise zu führen. Dabei werden wir insbesondere die Möglichkeiten einer datenschutzgerechten Verfahrensweise durch den Einsatz einer automatisierten Datenverarbeitung auch im Bereich der Arztgeschäftsstelle prüfen. Ohnehin wurde in unseren Gesprächen mit der Strafvollzugsanstalt und der Senatsverwaltung für Justiz deutlich, dass viele datenschutzrechtliche Probleme durch die Einführung eines automatisierten Datenverarbeitungssystems, das die datenschutzrechtlichen Gesichtspunkte berücksichtigt, lösbar wären.

Inhaftierte einer Berliner Justizvollzugsanstalt glaubten ihren Augen nicht zu trauen. Nachdem ein defekter Fernsehapparat gegen ein Ersatzgerät ausgetauscht worden war, begannen sie, mit der Fernbedienung die Programme neu einzustellen. Plötzlich sah ein Inhaftierter sich selbst auf dem Bildschirm. Nach kurzer Suche fanden die Inhaftierten im TV-Gehäuse eine stecknadelgroße Kamera.

Der Vorgang erregte auch in der Öffentlichkeit einiges Aufsehen. Die *Kamera* war in der *Justizvollzugsanstalt* im Zusammenhang mit einem Ermittlungsverfahren als Maßnahme nach § 100 c StPO installiert worden. Danach ist die Herstellung von Bildaufzeichnungen ohne Wissen des Betroffenen zulässig, wenn die Erforschung des Sachverhaltes auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Nach § 100 c Abs. 2 Satz 2 StPO dürfen sich die Maßnahmen auch gegen andere Personen richten, wenn die Erforschung des Sachverhaltes erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre.

Die Maßnahme war auch aus datenschutzrechtlicher Sicht zulässig und daher nicht zu beanstanden. Das Aufzeichnungsband ist bereits kurz nach dem Vorfall gelöscht worden.

4.3.2 Finanzen

Datenschutzkontrolle und Steuergeheimnis

Ein Petent beschwerte sich über ein Finanzamt. Nachdem wir das Finanzamt – unter Angabe der entscheidungserheblichen Umstände des Sachverhaltes – um eine Stellungnahme gebeten hatten, erhielten wir von der Senatsverwaltung für Finanzen die Mitteilung, eine Prüfung des

Einzelfalles sei ohne Übersendung einer Durchschrift der Eingabe des Steuerpflichtigen nicht möglich. Zur Begründung wurde darauf verwiesen, dass ansonsten nicht erkennbar sei, inwieweit der Einsender hinsichtlich einer Einzelauskunft eine wirksame Befreiung vom Steuergeheimnis (§ 30 AO) erteilt hat bzw. erteilen konnte. Im Übrigen könnten die landesgesetzlichen Regelungen im Berliner Datenschutzgesetz, die die Aufgaben und Befugnisse des Berliner Beauftragten für Datenschutz und Akteneinsicht definieren, die höherwertigen Regelungen im Bundesrecht (§ 30 Abs. 4 Nr. 2 AO) nicht durchbrechen.

Die uns übersandten Eingaben enthalten neben den entscheidungserheblichen Umständen des Einzelfalles vielfach vertrauliche Anmerkungen der Petenten (z.T. über Dritte) oder Ausführungen, die in der konkreten Angelegenheit nicht weiterführend sind. Nicht zuletzt um das in uns gesetzte Vertrauen der Petenten in eine unabhängige Bearbeitung und Bewertung der Angelegenheit rechtfertigen zu können, übersenden wir daher grundsätzlich keine Originale, Kopien oder Durchschriften der Eingaben an die speichernden Stellen.

Zum Spannungsverhältnis zwischen den datenschutzrechtlichen Kontrollbefugnissen und dem *Steuergeheimnis* hat der Gesetzgeber eine eindeutige Position bezogen. Nach § 28 BlnDSG besteht eine *Unterstützungspflicht* der Behörden und sonstiger öffentlichen Stellen des Landes Berlin gegenüber dem Berliner Beauftragten für Datenschutz und Akteneinsicht. Dieser Unterstützungspflicht haben die genannten Stellen unabhängig davon nachzukommen, welche Aufgaben ihnen nach Landes- oder Bundesrecht zugewiesen sind. In § 28 Abs. 2 BlnDSG ist klargestellt, dass Berufs- und Amtsgeheimnisse – egal aus welchem Gesetz (Bundes- oder Landesrecht) sich diese ableiten – die genannten Stellen nicht von ihrer Unterstützungspflicht entbinden. Die gilt auch für die Finanzbehörden des Landes Berlin und das Steuergeheimnis nach § 30 AO. Dem entspricht § 24 Abs. 2 BDSG, wonach dem Bundesbeauftragten für den Datenschutz gegenüber den öffentlichen Stellen des Bundes (z. B. dem Bundesministerium der Finanzen) eine Kontrollkompetenz auch in den Fällen eingeräumt wird, in denen personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 AO unterliegen, verarbeitet werden (§ 24 Abs. 6 BDSG erstreckt diese Regelung auch auf die Landesbeauftragten).

Erforderliche Angaben im Fahrtenbuch

Ein Petent hatte in seiner Einkommensteuererklärung ein Fahrtenbuch eingereicht, in dem nur die geschäftlich veranlassten Fahrten aufgeführt waren. Diese Angaben wurden vom Finanzamt als unzureichend abgelehnt.

Nach § 6 Abs. 1 Nr. 4 Satz 2 Einkommensteuergesetz (EStG) ist die private Nutzung eines betrieblichen/beruflichen Kraftfahrzeuges für jeden Kalendermonat mit einem Prozent des inländischen Listenpreises zum Zeitpunkt der Erstzulassung steuerlich zu berücksichtigen. Abweichend davon kann die private Nutzung mit den auf die Privatfahrten entfallenden Aufwendungen angesetzt werden, wenn die für das Kraftfahrzeug insgesamt entstehenden Aufwendungen durch Belege und das Verhältnis der privaten zu den übrigen Fahrten durch ein ordnungsgemäßes Fahrtenbuch nachgewiesen werden (§ 6 Abs. 1 Nr. 4 Satz 3 EStG). Die konkreten Anforderungen an die Führung eines Fahrtenbuches sind in einer Allgemeinen Verwaltungsvorschrift[101] geregelt. Daraus ergibt sich, dass ein *Fahrtenbuch* fortlaufend zu führen ist. Neben Datum und Kilometerstand zu Beginn und Ende jeder betrieblich/beruflich veranlassten Fahrt, Reiseziel, Reisezweck und aufgesuchtem Geschäftspartner müssen auch Angaben zu den dazwischenliegenden *Privatfahrten* enthalten sein. Für die Privatfahrten genügen jedoch die pauschalen Kilometerangaben. Angaben zum Zweck und Ziel der Privatfahrten werden vom Finanzamt nicht erwartet.

> *Im vergangenen Jahr*[102] *haben wir auf die rechtlichen Probleme hingewiesen, die bei der Führung von Fahrtenbüchern durch Ärzte, Rechtsanwälte, Steuerberater und andere zur besonderen Geheimhaltung verpflichtete Personen entstehen, wenn diese zum Nachweis der beruflichen Veranlassung der Fahrt den Zweck sowie die Namen und Adressen ihrer Patienten, Mandanten usw. anzugeben haben.*

Die mit dem Bundesministerium der Finanzen dazu geführte Diskussion führte zu einer datenschutzgerechten Lösung. Danach haben *Berufsgeheimnisträger* (z. B. Ärzte) zukünftig im Regelfall folgende Angaben zu beruflich/betrieblich veranlassten Fahrten in das Fahrtenbuch einzutragen: Zur Angabe „Reisezweck, -ziel, -route und aufgesuchter Geschäftspartner" reicht neben der Angabe des Datums, des Kilometerstandes und des Zielortes die Angabe „Patienten- bzw. Mandantenbesuch" als Reisezweck aus, wenn Name und Adresse des aufgesuchten Patienten oder Mandanten in einem vom Fahrtenbuch getrennt zu führenden Verzeichnis festgehalten werden. Es muss jedoch sichergestellt sein, dass die Zusammenführung von Fahrtenbuch und *Patienten- oder Mandantenverzeichnis* leicht möglich ist. Die Vorlage des Verzeichnisses soll vom Finanzamt nur verlangt werden, wenn tatsächliche Anhaltspunkte vorliegen, die Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen im Fahrtenbuch begründen und die Zweifel anders nicht auszuräumen sind.

---

101 Ertragssteuerliche Erfassung der Nutzung eines betrieblichen Kraftfahrzeuges zu Privatzwecken, zu Fahrten zwischen Wohnung und Betriebsstätte sowie zu Familienheimfahrten nach § 4 Abs. 5 Satz 1 Nr. 6 und § 6 Abs. 1 Nr. 4 Sätze 2 und 3 EStG vom 12. 5. 1997, Bundessteuerblatt I, S. 562

102 JB 1998, 4.3.2

4.3.2

Fehlerhafte Zustellung von Vollstreckungsankündigung

Ein Petent beschwerte sich bei uns über die Zustellungspraxis von Vollstreckungsunterlagen durch das Finanzamt. Er gab an, dass er seit längerer Zeit von seiner Ehefrau getrennt lebt. Obwohl die (neue) Anschrift seiner Ehefrau dem Finanzamt bekannt war, übersandte ihm das Finanzamt Schreiben mit Vollstreckungsankündigungen, die an seine Ehefrau gerichtet waren.

Die fehlerhafte Zustellung wurde von der Senatsverwaltung für Finanzen damit begründet, dass es technisch nicht möglich sei, bei getrennt lebenden Ehegatten verschiedene Anschriften zu speichern, wenn sie die Zusammenveranlagung zur Einkommensteuer gewählt haben und unter einer Steuernummer geführt werden. Da mit der *Vollstreckungsankündigung* Steuern eingefordert worden seien, die durch Veranlagung festgesetzt und gesamtschuldnerisch geschuldet werden, sah die Senatsverwaltung für Finanzen in dem Vorgehen keinen datenschutzrechtlichen Verstoß.

Hier irrt die Senatsverwaltung für Finanzen. Die Ehegatten haften zwar auch nach einer Trennung und der Wahl der Zusammenveranlagung zur Einkommensteuer dem Finanzamt gegenüber gesamtschuldnerisch; dies berechtigt jedoch bei der Durchführung von Vollstreckungsmaßnahmen gegenüber einem der beiden Ehegatten nicht, dem anderen Ehegatten Kenntnis hiervon zu geben. Die Mitteilung der neuen Wohnanschrift an das Finanzamt durch einen *getrennt lebenden Ehegatten* verdeutlicht, dass dieser auch unter seiner neuen Wohnadresse angeschrieben werden will. Da es sich hier nicht um einen Einzelfall handeln dürfte, haben wir gebeten, eine Umstellung des automatisierten Verfahrens vorzunehmen. Die Senatsverwaltung für Finanzen kündigte an, dass zu erwarten sei, dass das Problem (Erfassung von unterschiedlichen Adressen bei in Trennung lebenden Ehegatten trotz Zusammenveranlagung bei der Einkommensteuer) bei der Realisierung des Föderalen Integrierten Standardisierten Computerunterstützten Steuersystems (FISCUS) gelöst wird. Bis dahin werde eine „verstärkte personelle Überwachung“ derartiger Fälle eingeführt. Wir gehen davon aus, dass damit eine Anweisung und Überwachung der Sachbearbeiter gemeint ist, künftig in diesen Fällen die Schreiben an den jeweils Betroffenen zuzusenden.

Speicherung von Ermittlungsdaten bei Steuerstraftaten

Das Finanzamt für Fahndung und Steuerstrafsachen speichert in den Dateien FAHNKART und STRAKART sowie in einer „Namenskartei aller Beschuldigten und Betroffenen“ und den entsprechenden Akten personenbezogene Daten von in Steuerstrafverfahren Beschuldigten. Nach Auffassung der Senatsverwaltung für Finanzen ist Rechtsgrundlage für diese Datenverarbeitung (Speicherung für Zwecke künftiger Verfahren) § 88 a Abgabenordnung (AO).

In entsprechender Anwendung der Nrn. 4.1.21 und 4.1.26 der Anlage 1 zu den Aufbewahrungsbestimmungen der Berliner Steuerverwaltung (AufbewBest-St(Bln)) werden diese Daten nach Abschluss der Verfahren 10 Jahre (FAHNKART und STRAKART) bzw. 30 Jahre (Namenskartei) gespeichert. Diese Speicherfristen gelten ohne Berücksichtigung des Einzelfalles auch für Betroffene, bei denen der Tatverdacht sich nicht bestätigt hat, bei denen das Verfahren eingestellt oder die freigesprochen wurden.

§ 88 a Abgabenordnung (AO) löst ebenso wenig wie die §§ 88, 208, 385, 386, 404 AO i.V.m. der Strafprozessordnung (StPO) und der Buchungsordnung für die Finanzämter (BuchO) die Forderung des Volkszählungsurteiles nach einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entspricht, ein, denn sie regelt nicht hinreichend klar und für den Bürger verständlich, inwieweit personenbezogene Daten aus Steuerstrafverfahren unter welchen Voraussetzungen und zu welchem Zweck gespeichert und verarbeitet werden dürfen.

Die Vorschriften der AufbewBest-St(Bln) können nicht zu Eingriffen in Grundrechte der Betroffenen ermächtigen. Die Verarbeitung der Daten kann daher nur auf § 6 Abs. 2 BlnDSG i.V.m. §§ 13 bis 15 Bundesdatenschutzgesetz (BDSG) gestützt werden. Nach § 14 Abs. 1 BDSG ist das Speichern und Nutzen personenbezogener Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.

Die AufbewBest-St(Bln) differenzieren in keiner Weise nach dem Ausgang des gegen die Beschuldigten geführten Steuerstrafverfahrens. Es wird auch nicht die Erforderlichkeit der weiteren Speicherung geprüft, d. h. ob hinreichende tatsächliche Anhaltspunkte dafür bestehen, dass gegen die Betroffenen auch in Zukunft Steuerstrafverfahren geführt werden und die Kenntnis der alten Vorgänge für die Aufklärung der zu erwartenden neuen Straftaten erforderlich ist. Endet ein Steuerstrafverfahren mit einem rechtskräftigen Freispruch oder wird es nach § 170 Abs. 2 StPO eingestellt, besteht regelmäßig keine Erforderlichkeit der weiteren Erfassung der Daten der Betroffenen in Dateien des Finanzamtes für Fahndung und Steuerstrafsachen. Bei der Länge der Speicherfrist ist – soweit sich der Tatverdacht bestätigt hat – im Übrigen nach der Bedeutung der Straftat zu differenzieren. Bei Fällen von geringer Bedeutung ist die Frist angemessen zu reduzieren. Die pauschale Speicherungsdauer von 10 oder gar 30 Jahren ist zur Aufgabenerfüllung weder erforderlich noch angemessen.

Wir haben angeregt, die AufbewBest-St(Bln) so zu ergänzen, dass dem Recht der Betroffenen auf informationelle Selbstbestimmung Rechnung getragen wird. Dazu ist nach Abschluss eines Steuerstrafverfahrens zu prüfen, ob überhaupt eine weitere Speicherung personenbezogener Daten erforderlich ist. Soweit dies der Fall ist, ist eine Speiche-

rungsdauer festzulegen, welche sich an der Bedeutung des Straftatvorwurfes orientiert.

4.4 Sozialordnung

4.4.1 Arbeitnehmer und öffentliche Bedienstete

Der überwachte Arbeitnehmer

Mit dem zunehmenden Einsatz der Datenverarbeitung nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu, gleichzeitig steigern sich die Abhängigkeiten des Arbeitnehmers. Bereits lange vor Ausbreitung der modernen Informationstechnik in Betrieben und Verwaltungen hat sich die Rechtsprechung veranlasst gesehen, allzu weit gehenden Informationsanforderungen des Arbeitgebers entgegenzutreten und seinen Umgang mit arbeitnehmerbezogenen Daten zu reglementieren.

Auch die Datenschutzbeauftragten des Bundes und der Länder kritisieren bereits seit 1984[103], dass kein ausreichender Schutz für im Rahmen eines Arbeitsverhältnisses gesammelte Daten gewährleistet ist. Sie fordern daher seither die Schaffung eines einheitlichen speziellen Datenschutzgesetzes für Beschäftigte.

Auf eine Kleine Anfrage der SPD-Fraktion im Deutschen Bundestag im Jahr 1992 zu diesem Problem stellte die Bundesregierung klar, dass sie die Auffassung der Datenschutzbeauftragten teile und eine bereichsspezifische Regelung des *Arbeitnehmerdatenschutzes* ebenfalls für notwendig erachte[104]. Dennoch hat die Regierung bis zum heutigen Tag noch keinen Gesetzentwurf vorgelegt. Allerdings ist der Antwort der Bundesregierung auf eine Kleine Anfrage vom 1. September 1999 zu entnehmen, dass sie die Schaffung eines Arbeitnehmerdatenschutzgesetzes als dringlich ansieht und noch in dieser Legislaturperiode die Vorlage eines entsprechenden Gesetzentwurfs plant[105].

Im Rahmen des Arbeitsverhältnisses werden – anders als bei anderen Vertragsbeziehungen – personenbezogene Daten aus den verschiedensten Lebensbereichen des Arbeitnehmers erhoben. Diese Daten setzt der Arbeitgeber nicht nur für eigene Zwecke ein. An das Arbeitsverhältnis knüpfen auch Auskunfts-, Bescheinigungs- und Meldepflichten an, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, die anfallenden personenbezogenen Daten miteinander zu verknüpfen und sie losgelöst vom bisherigen Erhebungszweck für andere Verwendungen zu nutzen, entstehen Gefahren für das informationelle Selbstbestimmungsrecht des Arbeitnehmers.

---

103 JB 1984, 4.3
104 BT-Drs. 12/2948
105 BT-Drs. 14/1527

Der Einsatz von *Personalinformationssystemen* ermöglicht eine Systematisierung und Effektivierung der *Personalplanung* und des Personaleinsatzes. Durch Tastendruck können Arbeitgeber die verschiedenen Daten des Arbeitnehmers derart verknüpfen, dass ein Profil der Arbeitswilligkeit erstellt werden und bei der Personalplanung Berücksichtigung finden kann.

Zunehmender Beliebtheit bei Arbeitgebern erfreuen sich *Software-Produkte für Personal- und Organisationsentwickler* (SPO). Neu dabei ist die Verzahnung von Daten zu Mitarbeiterkompetenzen (Kompetenz-Profile), Weiterbildung/Training und Weiterbildungskosten. Mit Mouse-Klick beantwortet SPO Fragen nach den für die Tätigkeit erforderlichen und den tatsächlichen Kompetenzen der Mitarbeiter und beschreibt deren individuellen Fortbildungsbedarf. Eine Datenbank informiert, welche Kurse welche Kompetenzen fördern und welche Veranstalter diese Kurse anbieten. Aufgelaufene Kosten werden dabei ebenfalls automatisch verwaltet. Ähnliche Persönlichkeitsprofile werden immer häufiger auch bei Auswahlverfahren eingesetzt. Ausgeklügelte Verfahren der Bewerberauswahl bieten Orientierungshilfen, denn Fehlentscheidungen bei der Personalauswahl kommen Unternehmen teuer zu stehen.

Hinzu kommt, dass Arbeitnehmer zunehmend selbst Informationen automatisiert verarbeiten und damit Datenspuren in immer größerem Umfang hinterlassen[106]. Am *Arbeitsplatz* ist das Individuum umfangreichen Informationsanforderungen ausgesetzt. Betriebliche, unternehmerische und konzernweite *Vernetzungen* erlauben unternehmensübergreifend auch über die nationalen Grenzen hinweg die Sammlung und Übermittlung der durch die Nutzung entstehenden Daten.

So gewinnt die *Nutzung des Internet* zunehmend an Bedeutung. Insbesondere die Korrespondenz mittels E-Mail stellt eine Alternative zu anderen Übertragungsformen wie dem Telefax dar. Sie eröffnet allerdings dem Arbeitgeber den Zugang zum Kommunikationsverhalten der Arbeitnehmer. Amerikanische Firmen setzen immer häufiger Filtersoftware ein, mit der sie die elektronische Post ihrer Mitarbeiter kontrollieren. Dabei durchforsten Softwareprogramme die digitalen Botschaften nach sexuellen oder rassistischen Tabuwörtern oder Firmeninterna. Auch in Deutschland spähen Unternehmen ihre Mitarbeiter aus („Monitoring"). Sie setzen „Spitzel-Software" ein, mit der sie die Arbeitsleistung der Beschäftigten am Computer auf den Mouse-Klick genau erfassen und kontrollieren, ob und mit welcher Seitenauswahl sich der Angestellte während der Arbeitszeit ins WWW eingeloggt hat.

Auch *technische Überwachungseinrichtungen* mit Videokameras greifen im Arbeitsverhältnis in immer stärkerem Ausmaß um sich[107]. Warenverluste und damit finanzielle Einbußen werden von Arbeit-

106 JB 1998, 3.3
107 vgl. 3.1

gebern zum Anlass genommen, in Kunden- und Kassenräumen Videokameras zu installieren, um Straftaten zu verhindern bzw. zu erschweren und ggf. aufzuklären. Dass damit auch „Zeitdiebstähle" von Mitarbeitern aufgedeckt und die Wirtschaftlichkeit des Unternehmens durch gezielte Verhaltens- und Leistungskontrollen der Beschäftigten optimiert wird, ist nicht nur „lästiges Abfallprodukt", sondern bei etlichen Arbeitgebern erklärtes Ziel.

Soweit die offene, für jeden ersichtliche *Videoüberwachung ohne Aufzeichnung* nur als verlängertes Auge des Bewachungspersonals dient, ist sie unproblematisch. Da gesetzliche Regelungen zum Schutz der Arbeitnehmerinnen und Arbeitnehmer bei offener Videoüberwachung aber gänzlich fehlen, sollte in Betriebs- bzw. Dienstvereinbarungen klargestellt werden, dass die Überwachung nicht zur Verhaltens- und Leistungskontrolle dienen darf und Räumlichkeiten ohne Videoüberwachung für das Personal bereitgestellt werden müssen.

Das Sozialgericht München[108] *hatte 1990 über die Rechtmäßigkeit einer Sperrfrist nach dem Arbeitsförderungsgesetz zu befinden. Der Arbeitnehmer hatte mit seinem Arbeitgeber einen Aufhebungsvertrag mit sofortiger Wirkung geschlossen, da der Arbeitgeber im Ausstellungs- und Verkaufsraum eines Autohauses eine Videokamera installiert hatte, die Ton- und Bildaufnahmen fertigte. Das Sozialgericht entschied, dass die Sperrfrist zu Recht festgelegt wurde, da es dem Arbeitnehmer nicht unzumutbar war, seine Tätigkeit beim Autohaus fortzusetzen. Die Kamera war nämlich lediglich auf einen Teil des Austellungsraumes ausgerichtet. Damit war eine komplette Überwachung des Arbeitnehmers nicht gegeben. Vielmehr war das Verkaufsbüro, in dem der Schreibtisch des Arbeitnehmers stand und wo er auch die Verkaufsverhandlung abwickelte, nicht von der Kamera erfasst. Da somit keine „ständige, lückenlose" Videoüberwachung des Arbeitsplatzes stattfand, sah das Sozialgericht diese auch als für den Arbeitnehmer zumutbare Maßnahme an.*

Die Aufzeichnung von Bildern ist nur in Ausnahmefällen zulässig. Werden Aufzeichnungen angefertigt, so sind in einer Dienst- bzw. Betriebsvereinbarung Anlass der Aufzeichnungen, Zugriffsmöglichkeit, Verwendungszweck und Speicherdauer des Bildmaterials festzulegen.

Ganz anders ist der Fall zu beurteilen, wenn Arbeitnehmer mit *versteckter Videokamera* mit deren Kenntnis überwacht werden. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts liegt darin grundsätzlich ein rechtswidriger Eingriff in das Persönlichkeitsrecht des Beschäftigten. Der Eingriff in das Persönlichkeitsrecht des Arbeitnehmers, der darin besteht, dass er ohne konkreten Anlass zu jeder Zeit mit der Überwachung durch versteckte Kameras rechnen muss, kann allerdings durch die Wahrnehmung überwiegender schutzwürdiger Interessen des

108 RDV 1992, S. 85 ff.

Arbeitgebers gerechtfertigt sein. Zur Konkretisierung des Persönlichkeitsrechts bedarf es einer sorgfältigen Güter- und Interessenabwägung. Die Überwachung durch verdeckte Kameras ist dabei nur bei entsprechend gewichtigen schutzwürdigen Interessen und Pflichten des Arbeitgebers zulässig. Dazu bedarf es einer substanzierten Darlegung konkreter betrieblicher Beeinträchtigungen wie z. B. Warenverluste in nennenswertem Umfang etc., die einen so weit gehenden Eingriff des Arbeitgebers erforderlich machen. Voraussetzung ist ferner, dass der Einsatz von verdeckten Kameras die einzige Möglichkeit ist, weiteren Schaden zu verhindern bzw. zu begrenzen. Kann derselbe Erfolg auch mit weniger weit reichenden Mitteln, z. B. durch das Aufstellen von sichtbaren Kameras, herbeigeführt werden, so ist die Maßnahme unzulässig.

Erfolgt die Videoaufzeichnung dagegen nicht nur mit versteckter Kamera, sondern auch *ohne Wissen der Beschäftigten,* so müssen darüber hinaus zwei Voraussetzungen erfüllt sein, die einen so massiven Eingriff in das Persönlichkeitsrecht der Arbeitnehmer rechtfertigen. Zum einen muss der Einsatz der verdeckten Kamera die einzige Möglichkeit sein, einen mutmaßlichen Täter zu ermitteln, so dass die Aufstellung einer sichtbaren Kamera als weniger einschneidendes und milderes Mittel ausscheidet, und es muss vor Beginn der Maßnahme ein konkreter, durch nähere Anhaltspunkte begründeter Verdacht einer vorsätzlichen schweren Vertragsverletzung oder Straftat gegen einen oder mehrere Arbeitnehmer bestehen. Ein pauschaler Verdacht gegen die gesamte Belegschaft genügt regelmäßig nicht.

Stasi-Überprüfungen neu überdenken

Zehn Jahre nach dem Mauerfall mehren sich die Stimmen, die fordern, die *Regelüberprüfungen* von Mandatsträgern und Mitarbeitern im öffentlichen Dienst anhand von *Stasi-Unterlagen* zu überdenken und möglicherweise neu zu gestalten. So sagte der Regierende Bürgermeister Eberhard Diepgen bei einer Festveranstaltung am 9. November: „Zehn Jahre nach dem Mauerfall bin ich durchaus der Meinung, dass die Erkenntnisse der Gauck-Behörde nicht verschwiegen werden dürfen, aber im Hinblick auf ihre aktuelle Wirksamkeit den auch ansonsten üblichen Verjährungsfristen zu unterwerfen sind.“[109]

Auch die Datenschutzbeauftragten des Bundes und einiger Länder haben sich mit dem Thema befasst. Eine Einigung auf einheitliche Vorschläge kam nicht zu Stande, da auch hier über die weitere Vorgehensweise unterschiedliche Auffassungen bestehen.

Unsere Auffassung, die von den Landesbeauftragten in Brandenburg und Mecklenburg-Vorpommern geteilt wird, kommt in einem Papier zum Ausdruck, das den Datenschutzbeauftragten zur Diskussion vor-

[109] Berliner Zeitung v. 10. 11. 1999, S. 21

lag. Es umschreibt die Probleme, die hinsichtlich des künftigen Umfangs der Überprüfungen, der Nutzung der Daten, der Rechte der Betroffenen sowie der Aufbewahrung der Unterlagen insbesondere nach dem Ende des Jahres 2006 bestehen und wie sie gelöst werden könnten. Als Diskussionsgrundlage drucken wir das Papier im Anhang zu diesem Bericht ab[110].

Das 14-Augen-Prinzip

Gegen den Beamten einer Berliner Behörde wurden disziplinarische Vorermittlungen eingeleitet. Als Untersuchungsführer wurden zwei Juristen beauftragt. Da deren Abschlussbericht nicht die Billigung des Behördenleiters fand, bat dieser zwei weitere Beschäftigte um Überprüfung des Berichts in rechtlicher und tatsächlicher Hinsicht. Kurze Zeit später übersandte der Behördenleiter der Fachaufsicht den gesamten Disziplinarvorgang zur Übernahme, weil er sich für befangen erachtete. Da die Fachaufsicht dies zurückwies, erfolgte die formale Entbindung der bisherigen Vorermittlungsführer und die Einsetzung von zwei weiteren Juristen zur Fortführung des Vorermittlungverfahrens in der Dienststelle. Dabei handelte es sich bei dem einen um den behördlichen Datenschutzbeauftragten, der andere war bereits mit der Überprüfung des Berichts befasst gewesen. Im weiteren Verlauf wurden noch zwei Referendare mit dem Vorgang befasst. Letztlich waren allein in der Behörde sieben Personen mit der Bearbeitung des Disziplinarvorgangs beschäftigt. Dagegen beschwerte sich der Beamte.

Die Ermittlungsakten sowie der *Vorermittlungsbericht* der Untersuchungsführer sind Personalakten, die dem *Vertraulichkeitsschutz* des § 56 Abs. 1 Satz 1 Landesbeamtengesetz (LBG) unterliegen.

Der Grundsatz der Vertraulichkeit wird durch die Fürsorgepflicht des Dienstherrn nach § 42 LBG konkretisiert. Danach ist dieser verpflichtet, zur Wahrung der Rechte des Beamten den Kreis der mit Personalaktendaten Beschäftigten möglichst eng zu halten und auch Teilakten, Auszüge oder einzelne Angaben nicht ohne dienstlichen Grund – je nach dem Maße ihrer Schutzwürdigkeit – anderen Beschäftigten zur Kenntnis zu geben. Bei Vorermittlungsakten handelt es sich um besonders sensible Daten, bei denen dies in besonderem Maße gilt.

Selbst wenn man davon ausgeht, dass wegen des zu erwartenden Arbeits- und Zeitaufwandes die Beauftragung von zwei Vorermittlungsführern vom Behördenleiter für zweckmäßig erachtet wurde, war die Überprüfung des Ermittlungsergebnisses durch zwei weitere Personen nicht erforderlich, da der Bericht durch die eingesetzten Ermittlungsführer selbst hätte nachgebessert werden können.

110 Anlage 3

Noch problematischer ist die Beauftragung von zwei zusätzlichen Personen mit der weiteren Durchführung des Vorermittlungsverfahrens. Hinzu kam, dass einer der Beamten behördlicher Datenschutzbeauftragter war. Ein Datenschutzbeauftragter, der nebenher als Ermittlungsbeamter personenbezogene Angaben verwerten kann, die ihm nur als behördlichem Datenschutzbeauftragten zugänglich wären, kommt in Konflikt mit seiner Verschwiegenheitspflicht gemäß § 19 Abs. 5 BlnDSG i. V. m. § 36 Abs. 4 BDSG. Unabhängig von seinen subjektiven charakterlichen Eigenschaften steht damit seine Zuverlässigkeit im Sinne von § 36 Abs. 2 BDSG in Frage. Das Vertrauen, das der behördliche Datenschutzbeauftragte gerade bei jenen genießen muss, die Gründe haben, die datenschutzrechtlich korrekte Durchführung von disziplinarischen Vorermittlungen zu bezweifeln, könnte sich nicht einstellen. Damit wären aber die Voraussetzungen, das Amt als Datenschutzbeauftragter ordnungsgemäß auszuüben, entscheidend in Frage gestellt.

Auch die Übermittlung des gesamten Vorgangs an die Fachaufsicht war datenschutzrechtlich bedenklich. § 56 d Abs. 1 Satz 1 LBG bestimmt, dass es ohne Einwilligung des Beamten zulässig ist, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Soweit eine Auskunft ausreicht, ist aber von einer Vorlage abzusehen. Vorlage und Auskunft sind auf den jeweils erforderlichen Umfang zu begrenzen (§ 56 d Abs. 3 LBG). Diese Regelungen müssen auch für die Weiterleitung von Personalaktendaten an die weisungsbefugte Behörde im Rahmen eines Disziplinarvorgangs herangezogen werden. Die Übersendung des gesamten Vorgangs im Rahmen der Befangenheitsprüfung entspricht dem ersichtlich nicht, da sich die Befangenheit allein aus der Drohung mit einer Anzeige durch den Anwalt des Petenten ergeben sollte.

Die Tatsache, dass im weiteren Verlauf der Vorgang zusätzlich zwei noch in der Ausbildung befindlichen Juristen zur Bearbeitung überlassen wurde, ist mit der Geheimhaltungspflicht ebenfalls unvereinbar.

Übertriebener Diensteifer

Ein Beamter des Bundeskriminalamts suchte wegen eines Anfangsverdachts gegen eine Beamtin den Leiter der Personalabteilung eines Berliner Bezirksamts auf und bat um Einsichtnahme in die Personalakte. Der strafrechtliche Vorwurf hatte keinen Bezug zu der Amtstätigkeit der Beamtin. Diese wurde auch nicht von der Einsichtnahme bzw. Auskunftserteilung informiert. Der Leiter des Personalamts konnte sich im Nachhinein nicht mehr genau erinnern, ob er dem Beamten des Bundeskriminalamts die Personalakte zur Einsichtnahme überlassen oder nur einzelne Daten zum Lebenslauf und der Wohnanschrift zur Verfügung gestellt hatte.

4.4.1

Auskünfte aus der *Personalakte* dürfen 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 (§ 56 d Abs. 2 LBG). Inhalt und Empfänger der Auskunft sind dem Beamten schriftlich mitzuteilen. Die Auskunft ist auf den jeweils erforderlichen Umfang zu beschränken (§ 56 d Abs. 3 LBG).

Dies bedeutet, dass in jedem Einzelfall das konkrete Informationsbedürfnis des Datenempfängers Maßstab für den Umfang der zu übermittelnden Daten darstellt. Die ersuchte Behörde hat vor Weitergabe der Akten oder vor Erteilung einer Auskunft zu prüfen, ob die Erforderlichkeit der Akteneinsicht in dem erbetenen Umfang dargelegt ist. Ist für die ersuchte Behörde erkennbar, dass der Informationsbedarf auch anders gedeckt werden kann, so muss sie von einer Weitergabe der Akten absehen.

Hinzu kommt, dass die Erteilung einer Auskunft grundsätzlich an die Einwilligung des Beamten knüpft, es sei denn, dass ein gewichtiges vorrangiges Informationsinteresse des Dritten oder eine erhebliche Beeinträchtigung des Gemeinwohls die Auskunftserteilung ohne Einwilligung zwingend erfordert. Auch in diesen Fällen sollte aufgrund der Fürsorgepflicht des Dienstherrn versucht werden, zunächst die Einwilligung des Beamten einzuholen bzw. der Auskunftserteilung entgegenstehende Interessen festzustellen. In jedem Fall darf die Übermittlung der Daten nicht hinter dem Rücken des Beamten stattfinden. Er ist nach § 56 d Abs. 2 Satz 2 LBG über Inhalt und Empfänger der Auskunft schriftlich zu informieren.

Im vorliegenden Fall ist sowohl eine Interessenabwägung als auch eine schriftliche Benachrichtigung der Beamtin über die Einsichtnahme in ihre Personalakte bzw. Auskunftserteilung aus ihrer Personalakte an einen Beamten des BKA unterblieben.

Integrierte Personalverwaltung

Im Jahr 2000 soll die seit 1992 geplante *„Integrierte Personalverwaltung“* (IPV) in der Berliner Verwaltung sukzessiv in den Echtbetrieb gehen. Über die Entwicklung haben wir kontinuierlich berichtet[111].

Mit IPV soll die Personalverwaltung vereinfacht werden, indem verschiedene Funktionen von der Bearbeitung von Urlaubs- oder Teilzeitanträgen bis zu den Lohn- und Gehaltsbuchungen einzelner Stellen zusammengefasst werden. Weiterhin sollen Funktionen der Büroleitung, der Personalwirtschaftsstellen, der Personalaktenführung und

111 JB 1993, 4.5.1; JB 1996, 4.4.1; JB 1997, 2.3; JB 1998, 2.2

viele mehr zu einem Personalinformationssystem integriert werden. Realisiert wird IPV auf der Grundlage des Moduls Human Ressources (HR) eines *SAP R/3* Systems[112].

Erste Pilotanwendungen wurden frühzeitig in den Bezirken Köpenick und Wedding erprobt. Dabei lag bis März 1998 der Schwerpunkt auf der Personalverwaltung, während für die Zahlbarmachung der Löhne, Gehälter und Besoldung eine Schnittstelle zum Altverfahren des Landesverwaltungsamtes geschaffen werden sollte. Inzwischen ist der Funktionsumfang so erweitert worden, dass die Personalzahlungsverfahren in das SAP R/3-System einbezogen und die Altverfahren abgelöst werden können.

Diese Strategieänderung erfolgte gegen den Willen der mit der Anpassung des SAP-Systems an die Berliner Bedürfnisse (sog. *Customizing*) betrauten Unternehmensberatung, die daraufhin einseitig kündigte. Dies führte zu einer weiteren Verzögerung des Projekts, die durch den Einstieg der SAP AG selbst für das Customizing in Grenzen gehalten werden konnte.

Mit Auflösung der Projektgruppe IPV bei der Senatsverwaltung für Inneres und der Gründung des Service- und Systemunterstüzungscenters (SSC) beim *Landesverwaltungsamt* am 1. April 1999 ging das Verfahren aus der Projektierungs- in die Einführungsphase über. Das SSC ist seit diesem Zeitpunkt Verfahrensbetreiber. Im Zuge dieses Übergangs hatten wir die Änderungen der vorliegenden Konzeption zu bewerten.

Ein Schwerpunkt liegt auf dem *Sicherheitskonzept,* das von der Projektgruppe erstellt wurde und das u. a. das Berechtigungskonzept enthält. Die Ausgestaltung erfolgte datenschutzgerecht und unter Berücksichtigung der IT-Sicherheitsrichtlinie[113]. Offene Fragen wurden mit uns abgestimmt und gelöst.

Die Grundlage für das *Berechtigungskonzept* bildet eine fiktive Senats- bzw. Bezirksverwaltung, so dass bei der später erfolgenden Einführung in einer realen Verwaltung die Umsetzung des allgemeinen Sicherheitskonzepts auf die vorhandenen Infrastrukturen nochmals kritisch beobachtet werden muss. Als erste Senatsverwaltung soll im Mai 2000 die Senatsverwaltung für Inneres den Produktivbetrieb mit IPV aufnehmen. In einer Sitzung des Unterausschusses „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin gab die Senatsverwaltung für Inneres, die sich in Bezug auf die Umsetzung der IT-Sicherheitsrichtlinie für den IPV-Einsatz im eigenen Hause eher zurückhaltend geäußert hatte, die Zusage, rechtzeitig zum Beginn des Echtbetriebes ein Sicherheitskonzept umgesetzt zu haben.

---

112 JB 1998, 4.8.1

113 Richtlinie zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung v. 5. 1. 1999, DBI. l, Nr. 2, S. 5 ff.

4.4.2

Die hohe Schutzbedürftigkeit der Personaldaten veranlasste uns sehr frühzeitig, die *Verschlüsselung* der IPV-Daten während der Übertragung über das Berliner Landesnetz nachhaltig zu empfehlen. Da sich die Suche nach einem starken Verschlüsselungsprodukt, welches als Infrastrukturdienstleistung zentral vom Landesbetrieb für Informationstechnik und verfahrensunabhängig angeboten werden soll, erheblich hinzögerte, hätten wir nach dem Motto „Besser als gar nichts" übergangsweise auch eine schwächere Lösung akzeptiert. Allerdings wurden im Oktober 1999 erfolgreiche Tests mit einer starken Verschlüsselungssoftware am IPV-Verfahren durchgeführt, so dass dieses Problem zumindest für IPV eine Lösung finden wird[114].

4.4.2 Gesundheit

Gesundheitsreform 2000

Im Jahre 1999 wurde versucht, vieles im Gesundheitswesen zu bewegen. Die Bundesregierung nahm die *Gesundheitsreform 2000* in Angriff. Der Gesetzentwurf[115] wies allerdings erhebliche datenschutzrechtliche Mängel auf, die bei den Datenschutzbeauftragten des Bundes und der Länder und in der breiten Öffentlichkeit auf Kritik stießen.

Der Gesetzentwurf gab das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf, wonach aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung stehen. Geplant war, diese Informationen den Krankenkassen generell versichertenbezogen zu übermitteln. Es bestand die Gefahr des *„gläsernen Patienten"*. Das Arztgeheimnis wäre ausgehöhlt worden. Denn bei den gesetzlichen Krankenkassen wären Datenbestände aller gesetzlich Versicherten entstanden, aus denen sich für jeden einzelnen Patienten ein vollständiges Gesundheitsprofil hätte erstellen lassen. Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar war, in welcher Rechtsform (öffentlich-rechtlich oder privat) sie betrieben werden sollen, hätte eine weitere, krankenkassenübergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge gehabt (§ 294 SGB V des Entwurfs).

Wir haben Verständnis für die Bemühungen, die Kosten des Gesundheitswesens zu begrenzen, ohne gleichzeitig die gute Versorgung der Patienten zu verschlechtern. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, bei dem Eingriff in das Recht auf informationelle Selbstbestimmung die Erforderlichkeit und die Verhältnismäßigkeit zu

---

114 vgl. 4.8.2

115 Gesetzentwurf der Fraktionen der SPD und Bündnis 90/Die Grünen, BT-Drs. 14/1245, und der gleichlautende Gesetzentwurf der Bundesregierung, BT-Drs. 14/1721

wahren. Der Gesetzentwurf ließ jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die ohne die Speicherung umfangreicher Patientendatenbestände bei den Krankenkassen auskommen, ungeeignet sein sollten, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben dringend eine Überarbeitung empfohlen[116]. Der Gesetzentwurf wurde daraufhin wesentlich verbessert und weiterentwickelt. Die Krankenkassen sollten nunmehr von den Leistungserbringern (z. B. Ärzten, Krankenhäusern, Apotheken) die *Patientendaten* nicht mehr in personenbezogener, sondern in *pseudonymisierter Form* erhalten[117]. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen[118]. Als Folge der Kritik der Datenschutzbeauftragten wurden vom Bundestag auch die Regelungen zum Umgang mit den Daten der Versicherten in der gesetzlichen Krankenversicherung erheblich verbessert, z. B. durch die Beschränkung der Datenzugriffsrechte innerhalb der Krankenkassen[119] oder die Einführung eines Beratungsgeheimnisses[120].

Am 4. November 1999 hat der Bundestag das Gesundheitsreformgesetz in dieser Fassung, die sogar datenschutzrechtliche Verbesserungen gegenüber der bisherigen Rechtslage enthielt, beschlossen. Nachdem sich abzeichnete, dass der Bundesrat dem Gesetzentwurf nicht zustimmen und eine Abtrennung der zustimmungsbedürftigen Teile erfolgen würde, appellierten die Datenschutzbeauftragten an die zuständigen gesetzgebenden Körperschaften, die – politisch bisher völlig unstreitigen – datenschutzrechtlichen Teile im Bundesrat passieren zu lassen, da durch das „Aufschnüren“ des Paketes und die Preisgabe der zustimmungspflichtigen Teile des Gesetzes drohte, dass die datenschutzrechtlichen Verbesserungen nicht umgesetzt werden. Sie haben darauf hingewiesen, dass das bisherige Verfahren grundlegend verbessert würde, weil bei den Krankenkassen auch Krankenhaus- und Arzneimittelkosten nicht mehr personenbezogenen abgerechnet werden müssten.

---

116 Entschließung zu „Gesundheitsreform 2000“, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A II

117 Beschlussempfehlung und Bericht des Ausschusses für Gesundheit insbesondere zu § 294 SGB V, BT-Drs. 14/1977

118 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Patientenschutz durch Pseudonymisierung“, Anlagenband „Dokumente zum Datenschutz 1999“, Teil A III

119 Beschlussempfehlung und Bericht des Ausschusses für Gesundheit zu § 284 Abs. 4 SGB V, BT-Drs. 14/1977

120 Beschlussempfehlung und Bericht des Ausschusses für Gesundheit zu § 305 SGB V, BT-Drs. 14/1977

Während der Beratungen in den Ausschüssen des Bundestages wurde dieser versichertenfreundliche Gesetzesteil quer durch die Parteien befürwortet und so verabschiedet. Selbst die Kassen und die Pharmaindustrie begrüßten die Vorschläge weitgehend. Bedeutende zusätzliche Kosten wären durch das neue Verfahren nicht entstanden. Wir haben der Senatorin für Gesundheit und Soziales empfohlen, diesem Teil des Gesetzentwurfs im Bundesrat zuzustimmen. Leider wurde dem Appell der Datenschutzbeauftragten nicht gefolgt. Nach einer ablehnenden Stellungnahme des Bundesrates hat der Bundestag am 16. Dezember 1999 auf Beschlussempfehlung des Vermittlungsausschusses[121] das Gesetz zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 ohne die wesentlichen datenschutzrechtrechtlichen Verbesserungen beschlossen[122].

Gesundheitsdatengesetz

Auch außerhalb des Systems der gesetzlichen Krankenversicherung sind bundesgesetzliche Regelungen zur *medizinischen Datenverarbeitung* erforderlich. Die Europäische Datenschutzrichtlinie untersagt die Verarbeitung von personenbezogenen Daten über *Gesundheit* oder *Sexualleben,* wenn nicht bestimmte Ausnahmen vorliegen (Art. 8 Abs. 1). Hierzu gehören die ausdrückliche Einwilligung der betroffenen Patienten, die Datenverarbeitung auf dem Gebiet des Arbeitsrechts, der Schutz lebenswichtiger Interessen oder wenn der Betroffene außer Stande ist, die Einwilligung abzugeben, sowie der Umstand, dass die Daten von der betroffenen Person selbst offenkundig öffentlich gemacht worden oder sie zur Rechtsverfolgung erforderlich sind (Art. 8 Abs. 2).

Die Vorgaben des Artikels 8 der Richtlinie machen eine flächendeckende, sinnvollerweise bundesrechtliche Regelung des Umgangs mit *Gesundheitsdaten* erforderlich, die durch spezialrechtliche Regelungen auf Bundes- und Landesebene verfeinert werden kann. Es besteht erheblicher Regelungsbedarf in verschiedener Hinsicht. So wäre zu prüfen, ob Gesundheitsdaten generell unter einen besonderen Schutz zu stellen sind, ob ein Gesundheitsdatengeheimnis zu schaffen ist, ob überhaupt ohne explizite Einwilligung die Verarbeitung erlaubt werden darf, an welche Stellen Daten übermittelt werden dürfen, wie mit besonders sensiblen Daten umzugehen ist und welche angemessenen Garantien zur Sicherung der informationellen Selbstbestimmung im Zusammenhang mit anderen Daten gegeben werden müssen. Die Entwicklung neuer Techniken sowie Auskunfts- und Einsichtsrechte und der Aufbau von Gesundheitsregistern sowie die Verwendung von Gesundheitsdaten in Wissenschaft und Forschung, Ausbildung und Lehre bedürfen einer expliziten Regelung.

---

121 BT-Drs. 14/2369
122 BGBl. I 1999, S. 2626

Zwar sieht die Bundesregierung keine Veranlassung „ein übergreifendes Medizindatenschutzrecht in Form eines Rahmengesetzes“ vorzuschlagen[123]. Sie verweist vielmehr auf „bereichsspezifische Datenschutzvorschriften“. Dies kann aber nicht ausreichen, die Breite der Verwendung von Gesundheitsdaten abzudecken.

Approbation von Psychotherapeuten

Diskussionen verursachte die Approbation bzw. Zulassung der Psychotherapeuten nach dem Psychotherapeutengesetz, weil die Kassenärztliche Vereinigung zur Prüfung der fachlichen Kompetenz eine Anzahl von Fallbearbeitungen verlangte, die von den Antrag stellenden Therapeuten zu berichten waren. Diese waren erheblich verunsichert, weil sie befürchteten, selbst bei Fortlassung des Namens aufgrund der Gesamtumstände ohne Absicht doch Patientendaten zu offenbaren.

Wir haben den Therapeuten dringend nahe gelegt, bei der *Anonymisierung* ihrer Fälle so weit wie möglich zu gehen, damit auch im engeren Fachkreis nicht durch zufällige Bekanntschaften oder Vorkenntnisse eine Aufdeckung einer psychotherapeutischen Behandlung zu Lasten eines Patienten erfolgen würde. Zu bemängeln war an dem Verfahren nichts, weil die Kassenärztliche Vereinigung ausdrücklich auf die Angabe von personenbezogenen oder patientenbezogenen Daten verzichtet hatte. Es sollten lediglich Fallbeispiele aus der therapeutischen Praxis angeliefert werden.

Besuchskontrolle im Altenheim

Von einer Betreuungsperson wurde uns mitgeteilt, dass die Besucher an der Pforte eines Heimes und der zu besuchende Bewohner namentlich erfasst werden. Der Besucher wurde darüber nicht informiert; Gründe für die Speicherung wurden nicht angegeben. Die Pforte wurde auch nicht regelmäßig bewacht, so dass viele Besucher ohne Kontrolle und ohne notiert zu werden das Haus betreten konnten. Daraus ergab sich für einen Betreuer die missliche Situation, dass er in den Verdacht einer unregelmäßigen Abrechnung geriet. Denn ein Gericht, das die Abrechnung in einem Betreuungsverhältnis nachprüfen sollte, zog zum Beweis das Besucherbuch heran, wobei Unstimmigkeiten zwischen den im Besucherbuch eingetragenen Besuchen und dem Abrechnungsstand festgestellt wurden.

Das *Altenheim* war der Auffassung, diese Besucherliste aus Sicherheitsgründen für die Besucher und die Heimbewohner und für den Pflegebedarf führen zu müssen, weil die Befindlichkeit von Heimbewohnern oft von der Art des vorausgegangenen Besuches abhängig sei und zudem die Sicherheit der Besucher selbst geschützt werden sollte (z. B. bei Brandgefahr).

123 BT-Drs. 14/1527, S. 14

In der überwiegenden Zahl der Berliner *Pflegeheime* ist der freie Zutritt durch Besucher gewährleistet. Eine Kontrolle durch einen Pförtner erfolgt in der Regel nicht. Es gibt auch keine Kontrolle durch das Pflegepersonal in den einzelnen Wohnbereichen, mit der Ausnahme der normalen Beobachtung des Pflegeablaufs. Etwaigen Sicherheitsbedürfnissen der Heimbewohner kann durch den Heimbetreiber in Form einer Klingelanlage mit Wechselsprechanlage und entsprechenden Schließanlagen Rechnung getragen werden. Dem Willen der Heimbewohner ist Vorrang einzuräumen und sicherzustellen, dass diese jederzeit Besuch empfangen und das Heim verlassen können.

Die Heimbetriebe haben dafür zu sorgen, dass sich keine fremden Personen gegen den Willen der Heimbewohner Zugang zu den Bewohnerzimmern verschaffen. Hierzu ist es allerdings nicht erforderlich, die Häufigkeit der Besuche von Angehörigen, Betreuern oder anderen Personen zu erfassen. Eine derartige Regelung wird vom Landesamt für Gesundheit und Soziales als Einschränkung der Privatsphäre des Heimbewohners angesehen. Das Landesamt geht davon aus, dass auch die Pflegeheime diese Bewertung teilen. Denn die Heimverträge enthalten keine Berechtigung eines Heimes zu einer Protokollierung von Betreuerbesuchen. Meist ist sogar das Gegenteil der Fall, wonach durch eine Klausel die Erfassung bewohnerbezogener Daten begrenzt ist auf Daten, die zur Pflege und Betreuung benötigt werden, und dass diese Daten vertraulich zu behandeln sind. Eine Weitergabe solcher Daten an Dritte, mit Ausnahme an die Heimaufsicht und an den Medizinischen Dienst der Krankenkassen, erfolgt nicht.

Fallkonferenzen

Da wegen Sparmaßnahmen auch in psychiatrischen und geriatrischen Krankenhäusern Betten abgebaut werden müssen, stellt sich für eine ältere Person mit phasenweiser Verwirrtheit und ständigem Pflegebedürfnis die Frage nach dem Wohin.

Da die Pflege zum Teil durch die Sozialhilfe finanziert wird, schlägt die Sozialverwaltung *„betreutes Wohnen"* vor, bei dem privat organisierte Leistungserbringer die Pflege und Unterbringung kostengünstiger anbieten. Die Frage des „Wohin" wird in einer Fallkonferenz erörtert, wo sich sowohl Vertreter des Sozialpsychiatrischen Dienstes, des Krankenhauses, aber auch unterschiedliche Trägereinrichtungen einfinden, um eine angemessene Bleibe für den pflegebedürftigen Menschen zu finden.

Die *Fallkonferenz* wird auch unter anderer Bezeichnung tätig. Die regionalisierte „gemeindenahe", d. h. bezirkliche Versorgung *psychisch kranker Menschen* ist ein zentrales Ziel der Psychiatriepolitik im Lande Berlin. Um dieses Ziel zu erreichen, wurden in den Bezirken Plan- und Leitstellen und ein Psychiatriekoordinator eingerichtet, denen die Pla-

nung und Steuerung von psychosozialen Einrichtungen im gemeindenahen oder bezirklichen Bereich obliegen. Die Fallkonferenz steuert dabei die weitere Versorgung der einzelnen Patienten. Maßgeblich kommt es auf die individuelle Bedarfssituation der Patienten an.

Es stellt sich jedoch ein Datenschutzproblem insofern, als in der Fallkonferenz über die Persönlichkeit und das Leiden eines Patienten gesprochen werden muss, um dessen Versorgung so gut wie möglich zu gestalten. Die an uns herangetragenen Bedenken (gegenüber dieser „offenen" Situation) haben wir aufgegriffen, um in einer gemeinsamen Arbeitsgruppe mit der Senatsverwaltung für Gesundheit und Soziales unter Beteiligung der Bezirke bzw. freien Träger ein Konzept zu entwickeln, wie der Patientenschutz in diesem Gremium nachhaltig geschützt werden kann. Rechtliche Voraussetzung ist, dass der Patient diesem Verfahren zustimmt. Aber wesentlich ist vor allem, dass er oder sein Betreuer diese Zustimmung vor dem Hintergrund einer klaren Vorstellung von der Zusammensetzung der Fallkonferenz abgeben kann.

In einem Empfehlungsschreiben sollen die Bezirke modellhaft auf die bestehenden Interessenkonflikte hingewiesen werden. Die Fallkonferenzen sind so zu gestalten, dass eine Verletzung schutzwürdiger Belange der Patienten ausgeschlossen werden kann. Grundsätzlich muss jedoch von einer Mitwirkungspflicht und Mitwirkungsbereitschaft des Patienten an diesem Verfahren ausgegangen werden. Auf die Mitwirkung als tragendes Element der Sozialarbeit und des sozialen Leistungsrechts kann auch hier nicht verzichtet werden. In der Fallkonferenz soll durch einen Fürsprecher, der jeweils von Sitzung zu Sitzung bestimmt wird, sichergestellt werden, dass auch für nichtanwesende Patienten oder für solche Patienten, die ihre Interessen nicht mehr sachgerecht vertreten können, eine möglichst behutsame und angemessene Handhabung ihrer Lebens- bzw. Krankengeschichte erfolgt.

Prüfung der Arbeitsunfähigkeit

Eine Berliner Krankenkasse hat einen großen Teil ihrer Mitarbeiter auch krankenversichert. Betreut werden diese Mitglieder von einem Mitarbeiter dieser Krankenkasse in einem „Mitarbeiterkrankenbüro". Ein Petent war für längere Zeit arbeitsunfähig geschrieben, wurde jedoch kurz vor dem Ablauf des Arbeitsverhältnisses vom Arzt gesundgeschrieben, wodurch der Urlaubsanspruch erhalten blieb. Die Krankenkasse beauftragte daraufhin als Arbeitgeberin das Mitarbeiterkrankenbüro, die „Arbeitsfähigkeitsschreibung" ärztlich durch den Medizinischen Dienst der Krankenkasse nachzuprüfen. Der Anordnung lag wohl die Annahme zugrunde, dass durch die „Gesundschreibung" lediglich der Urlaubsanspruch des Petenten gerettet werden sollte.

Nach § 275 Abs. 1 Ziff. 3 SGB V sind die Krankenkassen verpflichtet, zur „Beseitigung von Zweifeln" an der *Arbeitsunfähigkeit* eine gutach-

terliche Stellungnahme des *Medizinischen Dienstes der Krankenversicherungen* einzuholen. Hier hatte der Arbeitgeber jedoch Zweifel an der *Arbeitsfähigkeit* geltend gemacht. Eine enge Interpretation des Wortlautes von § 275 SGB V trifft nicht die Bedeutung dieser Bestimmung. Denn die Aufgabe des Medizinischen Dienstes besteht darin, in dem Dreiecksverhältnis zwischen Arbeitgeber, Arbeitnehmer und Krankenkasse zu klären, auf welcher Sachverhaltsgrundlage wirklichkeitsgerechte Entscheidungen zu finden sind. Der Begriff „Zweifel an der Arbeitsunfähigkeit" deckt damit auch Zweifel an der Arbeitsfähigkeit ab, denn die „Arbeitsunfähigkeit" ist begrifflich die unmittelbare Kehrseite der „Arbeitsfähigkeit".

Die Rache des Gehörnten

Eine verheiratete Frau lebte mit einem anderen Mann zusammen mit der Absicht, sich scheiden zu lassen. Der verlassene Ehegatte versuchte dies mit allen Mitteln zu unterbinden. Eines Tages teilte er der Ehefrau mit, über vertrauliche Daten ihres neuen Lebenspartners zu verfügen. Er gab brisante Details preis und stellte in Aussicht, diese Daten weiterzuleiten. Die Frau begab sich in die ehemals gemeinsame Wohnung, um ihren Gatten zur Rede zu stellen und um ihn von seinem Vorhaben abzubringen. Dieser hielt ihr ein Dokument mit sehr sensiblen Daten vor, das keinen Briefkopf aufwies. Die Petentin geht davon aus, dass es sich um einen Auszug aus einer Krankenkassendatenbank bezüglich ihres neuen Lebenspartners handelte und dessen Krankheitsverläufe betraf. Der verlassene Ehemann war bei einer Rentenversicherungsanstalt beschäftigt.

Die Überprüfung hat ergeben, dass die Möglichkeit bestanden haben könnte, unter einer fingierten Anfrage der *Rentenversicherung* von der Krankenkasse Krankheitsdaten zum Schein für die Rentenversicherungsanstalt abzufragen. Eine endgültige Aufklärung war trotz eingehender Prüfung, die im Einvernehmen mit der betroffenen Krankenkasse durchgeführt wurde, nicht möglich. Da auch die streitenden Parteien nach ihrer ersten Wut zu einer friedlichen Verständigung neigten, wurde keine Strafanzeige erstattet und die Sache nicht weiterverfolgt.

Dieser Fall kennzeichnet die Schwäche von Datenverarbeitungssystemen, die keine *Zugriffskontrolle* durchführen und diese protokollieren. Nur so könnte man im Nachhinein klären, von wem und aus welchem Grund auf Daten zugegriffen wurde.

4.4.3 Sozial- und Jugendverwaltung

BASIS I – Die Technik entwickelt sich weiter, die Sicherheit auch?

Mit dem IT-Verfahren *BASIS I* wird seit einigen Jahren die Bearbeitung von Sozial- und Jugendhilfeangelegenheiten in den Bezirken und dem Landesamt für Gesundheit und Soziales erfolgreich unterstützt. In

der Entstehungsphase des Projektes haben wir beratend mitgewirkt[124]. Die seinerzeit für die Sicherheit des Verfahrens vorgesehene Konzeption haben wir akzeptiert.

Nun hat sich die Informationstechnologie auch in der Berliner Verwaltung weiterentwickelt. Das Verfahren BASIS I wird inzwischen mit anderen Systemplattformen betrieben. Der ursprüngliche DOS-Client wurde teilweise durch eine grafische Benutzeroberfläche (WINDOWS 3.1) erweitert und verbessert oder durch ein moderneres Betriebssystem ersetzt. Mit diesen neuen Errungenschaften entstanden aber auch neue Risiken, die bei der ursprünglichen Konzeption noch nicht bedacht werden konnten und mussten. Es ist daher wichtig, die Sicherheitskonzepte an die neuen Gegebenheiten anzupassen bzw. neu zu entwickeln.

Wir haben daher in mehreren Bezirksämtern angekündigte Kontrollen des technisch-organisatorischen Datenschutzes bzw. der IT-Sicherheit durchgeführt. Die Kontrolle konzentrierte sich dabei auf Maßnahmen zur Zugangs-, Datenträger-, Speicher-, Benutzer- und Zugriffskontrolle einschließlich der Regelungen zum Umgang mit Passwörtern. Dabei gelangten wir zu folgenden Erkenntnissen:

Der Grad der *Vernetzung* in den Bezirksämtern ist in den letzten Jahren signifikant gewachsen. Mittlerweile sind die zahlreichen kleinen Einzelnetze jeweils zu einem bezirklichen Gesamtnetz zusammengefasst worden. Durch diese Entwicklung kann die IT-Kompetenz an einer zentralen Stelle konzentriert werden, was nicht nur wirtschaftlich vernünftig, sondern auch in Hinblick auf die IT-Sicherheit vorteilhaft ist, weil sich besser qualifizierte IT-Fachleute auch besser um die Sicherheitsfragen kümmern können.

Andererseits wird die *Zugangskontrolle* durch die enorme Zunahme von Klienten-PCs problematischer, da der Zugriff auf BASIS theoretisch von allen Arbeitsplatzrechnern im Bezirk möglich ist. Es ist daher wichtig, dass andere Schutzmaßnahmen, z. B. die der Speicher-, Benutzer- und Zugriffskontrolle, besonders wirksam sein müssen.

Ein weiterer Vorteil der Zusammenschaltung der bezirklichen Netze liegt darin, dass die bis dahin dezentral verteilten Server jetzt in einem zentralen, gut zu sichernden *Serverraum* untergebracht werden können. Allerdings mussten wir feststellten, dass diese zentralen Serverräume in mehr als der Hälfte der geprüften Bezirksämter Mängel der Zugangskontrolle aufwiesen. Beispielsweise werden die Server zusammen mit anderen schutzbedürftigen technischen Systemen, z. B. der Telefonanlage, untergebracht, bei deren Wartung und Betreuung Personen Zugang bekommen können, die nicht der IT-Stelle, meist sogar Fremdfirmen, angehören. Die notwendige Aufsicht durch die IT-Stelle wird meistens nicht gewährleistet.

---

124 vgl. u. a. JB 1994, 4.11

4.4.3

Die Forderung der früheren BASIS-Projektgruppe, vor dem Echteinsatz des Verfahrens ein eigenständiges *lokales Sicherheitskonzept* und die notwendigen Arbeitsanweisungen zum Datenschutz erstellt und umgesetzt zu haben, haben nur wenige Bezirksämter befolgt. Die frühere BASIS-Projektgruppe der Senatsverwaltung für Gesundheit und Soziales hatte Mustervorgaben für die Entwicklung solcher Konzepte und Anweisungen erarbeitet und mit uns abgestimmt. Für das damalige Pilotbezirksamt wurden die Mustervorgaben am Beispiel konkretisiert. Umso verblüffender war es für uns, als uns in einem Bezirksamt nach langem Praxiseinsatz von BASIS I erklärt wurde, für die Erstellung von Konzepten und Anweisungen warte man noch auf Vorgaben der Innenverwaltung.

Schon mehrfach wurde das Problem aufgeworfen, dass es bei der Client-Server-Anwendung BASIS I in bestimmten Fällen möglich ist, als normaler Anwender auf die *Betriebssystemebene* zu gelangen, womit die softwareseitigen Schutzmaßnahmen des Anwendungsverfahrens umgangen werden können. Die Projektgruppe hatte zu diesem Problem eine zufrieden stellende Lösung entwickelt und an die einsetzenden Stellen weitergegeben. Dies war Teil des Sicherheitspakets für BASIS I. Leider war nur ein einziges der besuchten Bezirksämter in der Lage, die Hinweise umzusetzen. Alle anderen nahmen diese Sicherheitslücke billigend in Kauf.

Die Entwicklung und Einführung modernerer Betriebssysteme (etwa WINDOWS 95, 98 und NT) hat diese Problematik leider verschärft. Sie bieten neben einer Fülle neuer Funktionen, die dem Anwender das Leben erleichtern können, leider auch neue Möglichkeiten, die bisher erfolgreich verwendeten Sicherheitsmaßnahmen zu umgehen. Dies zeigt, dass mit der Einführung modernerer Systemplattformen die bestehenden Sicherheitskonzeptionen neu bewertet und ggf. angepasst werden müssen. Aufgrund der jeweils eigenen Verantwortung für den sicheren und datenschutzgerechten Einsatz der Verfahren reicht es nicht, auf eventuelle Vorgaben zentraler Stellen zu warten. Es kann sich fatal auf die Verfahrenssicherheit auswirken, wenn die Sicherheitskonzepte nicht mit den Systemen mitwachsen.

Das beste Sicherheitskonzept nützt wenig, wenn es nicht konsequent umgesetzt wird. Die Voraussetzung dafür ist, dass die Nutzer vernünftig geschult werden, auch in der Beachtung von Sicherheitsregeln. Die Realität sieht leider in vielen Ämtern anders aus. Rechner und Programme können von knappen Mitteln bezahlt werden, die *Schulung* wird häufig genug eingespart. Neue Mitarbeiter werden entweder im „Crashkurs“ durch die IT-Stelle oder durch Kollegen eingewiesen. Schulungen, die u. a. auch die Beachtung von Sicherheitsrichtlinien vermitteln sollen, werden eher selten gewährt. Aber selbst dann, wenn gut geschult wurde, fehlten den Anwendern oft Unterlagen wie z. B. Benutzerhandbuch, in denen im Zweifel nachgeschlagen werden kann.

Sicherheit fängt im Bewusstsein des Anwenders an. Beim bloßen Unterzeichnen von Verpflichtungserklärungen, deren Inhalt schon nach wenigen Wochen in Vergessenheit gerät, kann man es nicht belassen.

Zusammenfassend ergab die Prüfung, wie auch Kontrollen und Erfahrungen bei vielen anderen Verfahren zeigen, dass zwar viele Ressourcen in die Automatisierung von Arbeitsabläufen investiert werden, wobei der praxistaugliche – genauer: anfangs fehlerarme – Einsatz als oberstes Ziel angesehen wird, andere wichtige Dinge, von denen auf Dauer der ordnungsgemäße und sichere Einsatz der Verfahren zwingend abhängt, wie Sicherheitskonzepte, Dokumentationen oder Benutzerhandbücher, aber auf einen unbestimmten späteren Zeitpunkt („Wenn man mal Zeit oder Geld hat!“) verschoben werden.

Amtsermittlung bei Sozialbehörden

In einem Sozialleistungsverfahren (laufende Unterstützung zum Lebensunterhalt) musste ein Bezirksamt in Erfahrung bringen, ob ein Hilfeempfänger mit einer anderen Person in eheähnlicher Lebensgemeinschaft gelebt hatte, wobei beide Partner inzwischen verheiratet sind. Gleichwohl wurde von beiden die vorherige eheähnliche Lebensgemeinschaft bestritten.

Die daraufhin vorgenommene Ermittlung bei *Nachbarn* war zulässig. Schon das Verwaltungsgericht hatte in einem hierauf bezogenen Verfahren durch Beschluss festgestellt, dass das Bezirksamt verpflichtet ist, eine solche Vorklärung auch bei Nachbarn durchzuführen, und hat dem Bezirksamt eine dementsprechende Auflage erteilt. Die Rechtsgrundlage für eine solche Untersuchung ergibt sich aus § 20 Abs. 1 i. V. m. § 69 Abs. 1 Ziff. 2 SGB X. Nach § 20 Abs. 1 SGB X hat die Behörde den Sachverhalt von Amts wegen zu ermitteln. Sie bestimmt Art und Umfang der Ermittlungen. Sie ist an das Vorbringen und an die Beweisanträge der Beteiligten nicht gebunden.

Dieser *„Untersuchungsgrundsatz“* scheint mit dem *Mitwirkungsgrundsatz* nach § 60 SGB X im Widerspruch zu stehen. Die Lösung der scheinbaren Widersprüchlichkeit ergibt sich aus den unterschiedlichen Zielsetzungen, die beiden Vorschriften zugrunde liegen. Während sich der Mitwirkungsgrundsatz auf die Obliegenheit des Hilfeempfängers bezieht, die für die Leistungsgewährung notwendigen Tatsachen selbst vorzutragen und glaubwürdig zu machen, betrifft der Untersuchungsgrundsatz die Befugnis der Behörde, einen Sachverhalt im öffentlichen Interesse aufzuklären. Ein öffentliches Interesse ist dann gegeben, wenn die Geltendmachung eines Erstattungsanspruchs oder die Androhung einer Sanktion in Aussicht steht. Die Verhinderung des Unterstützungsbetruges ist ein wesentlicher Teilaspekt der Leistungsfunktion der Sozialbehörden, die damit einen wesentlichen Beitrag zur sozialen Leistungsgerechtigkeit erbringen müssen.

Daraus ergibt sich, dass die Sozialbehörden verpflichtet sind, einen Sachverhalt von Amts wegen aufzuklären, wenn er durch die Mitwirkung des Hilfeempfängers aufgrund der zuwiderlaufenden Interessenlage, insbesondere wenn sich der Hilfeempfänger gegen eine weitere Aufklärung des Sachverhaltes sperrt, nicht aufgeklärt werden kann.

Geschwärzte Kontoauszüge

Ein Hilfeempfänger erhielt ergänzende Sozialhilfe. Hierzu musste er jeden Monat seine Kontoauszüge ungeschwärzt abliefern. Obwohl er mehrmals nach der gesetzlichen Grundlage gefragt hatte, wurde er nur auf seine Mitwirkungspflicht nach dem Sozialgesetzbuch hingewiesen. Der Hilfeempfänger wollte nicht einsehen, dass alle seine Geldeingangs- und -ausgangsdaten kontrolliert wurden, weil es doch seine Privatsache sei, für welchen Betrag er als Sozialhilfeempfänger telefoniere oder sich etwas auf Raten kaufe oder gar für welche Parteien oder Vereine er seine Mitgliedsbeiträge bezahle.

Eine allgemeine Richtlinie, in welchem Umfang *Kontoauszüge* vorzulegen sind, gibt es nicht. Die individuelle Einzelfallüberprüfung obliegt dem Ermessen der Mitarbeiter. So wird bei einem Erstantrag auf Sozialhilfe grundsätzlich die Vorlage ungeschwärzter Kontoauszüge der letzten drei Monate verlangt, denn vom Nachrangprinzip der Sozialhilfe ausgehend soll vermieden werden, dass durch das „Abräumen" der Konten bzw. durch das „Verlagern" von Geldern die Sozialhilfebedürftigkeit früher einsetzt als dies bei wirtschaftlichem Verhalten gegeben wäre. Ein weiterer Aspekt ist – je nach Einzelfall – die Erfüllung der Nachweispflicht bei den Zahlungen für Miete, BEWAG/GASAG, Krankenkasse, Schuldentilgung usw. Während des laufenden Bezuges von Sozialhilfe werden ungeschwärzte Kontoauszüge nur in bestimmten Einzelfällen, die Anlass zu einer eingehenden Prüfung gegeben haben, angefordert, z. B. um Rückstände von Mieten, Krankenkassenbeiträgen, unwirtschaftliches Verhalten oder den Verdacht von Sozialhilfebetrug zu ermitteln.

Allerdings ist trotz des legitimen Aufklärungsinteresses der Sozialbehörde auch ein *Geheimhaltungsschutz* anzuerkennen. So sollte dem Hilfeempfänger die Möglichkeit belassen werden, z. B. die Mitgliedschaft in politischen Parteien oder in Vereinen, für die möglicherweise auf dem Konto Beträge abgebucht werden, gegenüber dem Amt geheim zu halten. Auch ob er angemessene Kleinbeträge in dem einen oder anderen Geschäft ausgegeben hat, ist für das Sozialamt nicht entscheidungsrelevant. Solche Angaben sollten also in jedem Falle geschwärzt werden dürfen.

Echtdaten zur Programmentwicklung

Das Bezirksamt Neukölln teilte uns als Pilotbezirksamt für das zukünftige automatisierte Sozialhilfeverfahren BASIS II mit, dass es auf Bitte des mit der Entwicklung des Verfahrens beauftragten Konsortiums zweier Softwareunternehmen diesem den gesamten Datenbestand aus dem alten Verfahren PROSOZ (BASIS I) zur Entwicklung der Migrationssoftware für die Migration der Daten in das neue System zur Verfügung gestellt hat.

Die Bereitstellung der Daten an das Konsortium wurde als Lieferung zur Auftragsdatenbearbeitung beschrieben. Im vorliegenden Fall handelte es sich jedoch nicht um einen Auftrag, der von § 80 SGB X erfasst wird. Er betraf eben nicht die Verarbeitung oder Nutzung personenbezogener Sozialdaten, sondern die Entwicklung eines Programms zur Verarbeitung personenbezogener Daten. Die Entwicklung von Programmen fällt nicht unter die Aufgaben, die unter Anwendung von § 80 SGB X oder § 3 BlnDSG vergeben werden können. Nur die *Migration* selbst könnte als Datenverarbeitung im Auftrag zu betrachten sein.

Die beabsichtigte Verwendung der Daten durch das Konsortium ist als Nutzung der Sozialdaten anzusehen. Nach § 67 b i.V.m. § 67 c Abs. 1 SGB X ist dies nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben nach dem Sozialgesetzbuch erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind. Dies trifft für die Entwicklung eines Programms nicht zu.

Aus all dem folgt, dass die in Auftrag gegebene Verarbeitung oder Nutzung personenbezogener Daten unzulässig war, da keines der im SGB X beschriebenen Zulässigkeitskriterien für die Verarbeitung erfüllt war. Die Daten wurden zweckentfremdet verarbeitet bzw. genutzt.

Wir haben empfohlen, das Konsortium anzuweisen, die rechtswidrig bereitgestellten Daten unverzüglich zu löschen und alle bereits vorliegenden Arbeitsergebnisse mit personenbezogenen Daten zu löschen bzw. zu vernichten. Darüber hinaus ist für die Entwicklung der Migrationssoftware ein *Testdatenbestand* bereitzustellen, der keine personenbezogenen Echtdaten enthält. Der Testdatenbestand ist entweder auf der Grundlage der Dokumentation des Datenmodells für BASIS I zu entwickeln oder von den Betreibern des IT-Verfahrens PROSOZ/BASIS I durch eine geeignete Anonymisierung der Datensätze aus dem Echtdatenbestand abzuleiten. Das Bezirksamt Neukölln hat uns inzwischen mitgeteilt, dass das Konsortium die Daten gelöscht hat, nachdem es aufgrund unserer Beanstandung vom Bezirksamt dazu aufgefordert wurde.

4.4.3

Datenerhebung Jugend und Sucht

Die Drogenbeauftragte des Senats bei der Senatsverwaltung für Schule, Jugend und Sport beabsichtigte, ein IT-gestütztes Berichterstattungsverfahren für die Aktivitäten der Drogenberatungsstellen einzuführen. Dazu sollte der in den Drogenberatungsstellen erhobene und bundesweit einheitlich verabredete „Deutsche Kerndatensatz zur Dokumentation im Bereich der Suchtkrankenhilfe" in anonymisierter Form von den Drogenberatungsstellen an die Senatsverwaltung übermittelt werden.

Diese selbstverständlich zulässige anonyme Berichterstattung betrifft außerordentlich sensible personenbezogene Daten. Wird ruchbar, dass Daten, die Hilfe suchende Suchtkranke in den *Drogenberatungsstellen* preisgeben müssen, bei der Drogenbeauftragten zu einem nicht hinreichend anonymisierten „Suchtkrankenregister" konzentriert werden, so könnte dieser Vertrauensbruch das System der Drogenberatung zerstören.

Wir hatten die Prüfung angeregt, ein vollständiges *Anonymisierungsverfahren* zu benutzen, obwohl damit Doppelerfassungen unerkannt blieben und die Zuordnung von Datenänderungen ausgeschlossen würde. Dieses ist möglich, wenn die statistisch aufbereiteten und aggregierten Ergebnisse dadurch keine signifikante Verfälschung erleiden würden. Dies war jedoch aus Sicht der Drogenbeauftragten nicht akzeptabel, so dass es jetzt auf eine zuverlässige *Pseudonymisierung* ankam, die sowohl Doppelerfassungen anonym erkennbar machen als auch spätere Änderungen der richtigen Person zuordnen lassen würde.

Gegen den ursprünglichen Plan, einen Code zu verwenden („HIV-Code"), der aus Buchstaben und Zahlen zusammengesetzt ist, die sich mit einer eindeutigen Regel aus den vier Merkmalen Vorname, Nachname, Geschlecht und Geburtsjahr ermitteln lassen, hatten wir erhebliche Bedenken. Mit diesen vier normalerweise nicht vertraulich gehaltenen und nach Vorlage des Personalausweises bekannten Merkmalen lässt sich leicht das Pseudonym brechen.

Die Drogenbeauftragte hat dann ein Modell vorgeschlagen, mit dem wir uns einverstanden erklären konnten: Die Beratungsstellen erfassen die Einzelfälle personenbezogen und ordnen ihnen zwei Ordnungsmerkmale zu: Den HIV-Code mit bekanntermaßen nicht hinreichender Pseudonymisierungswirkung zur Identifizierung gleicher Fälle und eine interne Fallnummer. Die Beratungsstellen übermitteln der Drogenbeauftragten einen Datenträger mit den anonymisierten Einzelfällen und dem Ordnungsmerkmal „Interne Fallnummer". Gleichzeitig übermitteln die Beratungsstellen einer im Auftrag tätigen Abteilung des Robert-Koch-Instituts in Berlin einen Datenträger, der zu jedem Einzelfall den HIV-Code, die interne Fallnummer sowie die Kennung der Beratungsstelle, sonst aber keine Daten des Einzelfalls enthält. Das Robert-Koch-Institut ordnet jedem HIV-Code eine sog. Personennummer zu. Diese

Nummer wird so erzeugt, dass ein Rückschluss auf den HIV-Code über die Nummer ausgeschlossen ist. Diese Zuordnung bleibt im Robert-Koch-Institut gespeichert. Das Robert-Koch-Institut erzeugt schließlich einen Datenträger, der pro Fall nur die interne Fallnummer, die Personennummer und die Kennung der Beratungsstelle enthält, und übersendet diesen Datenträger an die Drogenbeauftragte.

Damit erhält die Drogenbeauftragte die hinreichend anonymisierten Falldaten und kann über die Personennummer die Daten zu den gleichen Personen zusammenführen. Das Robert-Koch-Institut kann zwar zu Personen, über deren Identifikationsdaten es verfügt, die Personennummer ermitteln, verfügt jedoch nicht über die eigentlichen Falldaten. Mit diesem Verfahren halten wir die Anonymität der bei der Drogenbeauftragten zu führenden Basisdokumentation für hinreichend gewährleistet.

Querschnittscontrolling

Im Zuge der Verwaltungsreform sollen auch Methoden des *Querschnittscontrollings* (QC) eingeführt werden. Aus einem Gutachten einer Unternehmensberatung für die Senatsverwaltung für Finanzen wird deutlich, dass in der QC zunächst Kriterien, Parameter und Rahmenbedingungen herausgearbeitet werden müssen, welche das staatliche Handeln in den vom Controlling[125] erfassten Aufgabengebieten steuern, und dann herausgefunden werden muss, welche Ausprägungen diese Kriterien, Parameter und Rahmenbedingungen haben müssen, damit das staatliche Handeln auch effektiv ist.

Die Verwaltung will somit verbesserte Steuerungsmöglichkeiten staatlichen Handelns durch ein integriertes Berichtswesen erproben und muss dazu vorher die optimalen Berichtsinhalte ermitteln.

Das QC wird in einem Pilotprojekt erprobt. Dafür wurde das sozialpolitische Programm *„Integration durch Arbeit – IdA“* im Geschäftsbereich der Senatsverwaltung für Gesundheit und Soziales ausgewählt. Dabei handelt es sich um ein Programm zur Umsetzung der Sozialleistung „Hilfe zur Arbeit“ (HzA) nach §§ 18 bis 20 BSHG. Bei der HzA geht es darum, geeignete Sozialhilfeempfänger wieder in den Arbeitsprozess einzugliedern und somit von der Sozialhilfe unabhängig zu machen. Pilotbezirke sind Köpenick und Neukölln.

Das QC bei IdA soll Kriterien liefern, unter welchen Umständen die Integration durch Arbeit erfolgreich und gleichzeitig in effektiver, d. h. Kosten sparender Weise erfolgen kann. Mit den außerordentlich sensiblen Daten, die zur Bewertung der Eingliederungsfähigkeit eines

[125] Man beachte, dass im Englischen Controlling weniger „Kontrolle“ als vielmehr „Steuerung“ oder „Lenkung“ bedeutet!

Sozialhilfeempfängers in den Arbeitsmarkt erforderlich sind, war ausgerechnet ein datenschutzrechtlich besonders heikles Arbeitsgebiet für das Pilotprojekt ausgewählt worden.

Für das IdA-Querschnittscontrolling wurde durch ein Beratungsunternehmen ein IT-Verfahren konzipiert, mit dem eine dezentrale Fallerfassung in den beteiligten Bezirken und eine zentrale Auswertung durch die Senatsverwaltung für Gesundheit und Soziales erfolgen sollte.

Das Querschnittscontrolling ist als *Organisationsuntersuchung* anzusehen, das seine Rechtsgrundlage in § 67c Abs. 3 Sozialgesetzbuch X findet, sofern

- für die Fallerfassung keine zusätzlichen Daten erhoben werden;
- sich der Zugriff auf die personenbezogenen Daten der Betroffenen an den dezentralen Arbeitsplätzen auf jene Mitarbeiter beschränkt, die für die Gewährung der Sozialleistungen bei der Hilfe zur Arbeit zuständig sind und daher ohnehin auf die Daten in den Akten zugreifen können;
- die Auswertung der dezentral erfassten und über das Berliner Landesnetz übertragenen Daten anonym erfolgt und diese demzufolge nur anonymisiert oder pseudonymisiert zum zentralen Server übertragen und dort verarbeitet werden.

Die letzten beiden Anforderungen gingen in das IT-Sicherheitskonzept für das IT-Verfahren ein. Das Konzept sieht vor, dass vor der Übertragung der Daten die identifizierenden Daten der Datensätze mit einem sicheren symmetrischen *Verschlüsselungsverfahren* verschlüsselt und damit für die Senatsverwaltung unlesbar gemacht werden. Dabei ist sicherzustellen, dass der Empfänger den Schlüssel nicht erhält. Da die Pseudonymisierung immer mit dem gleichen Schlüssel erfolgt, kann auch sichergestellt werden, dass spätere Datenänderungen oder -ergänzungen an den Datensätzen vorgenommen werden können, ohne dass gegenüber der Senatsverwaltung die Pseudonymität aufgehoben wird. Da die Daten für Dritte pseudonym sind, ist eine weitere Verschlüsselung für die Datenübertragung entbehrlich.

4.4.4 Bauen und Wohnen

Die Regenwasserabgabe und ihre Folgen

Auf das geplante Vorhaben der Berliner Wasserbetriebe (BWB), zukünftig ein getrenntes Entgelt für Schmutz- und Niederschlagswasser zu erheben, haben wir bereits in unserem letzten Jahresbericht hingewiesen[126]. *Im vergangenen Jahr wurden von den BWB die Erfassungsblätter an die*

126 JB 1998, 4.6.3

einzelnen Grundstückseigentümer mit der Bitte um eventuelle Berichtigung oder Vervollständigung versandt. Viele Bürger haben sich – gerade auch vor dem Hintergrund der Debatte um die Privatisierung der BWB – daraufhin an uns gewandt und äußerten die Befürchtung, dass nunmehr jedes beliebige private Unternehmen in den Besitz der Daten und Luftbildaufnahmen ihres Grundstücks gelangen könnte.

Die BWB sind auch nach ihrer Teilprivatisierung in der Rechtsform einer Anstalt des öffentlichen Rechts organisiert und damit nicht einem Privatunternehmen gleichzusetzen. Als Unternehmen der öffentlichen Energie- und *Wasserversorgung* können die BWB zur Erfüllung ihrer Aufgaben Angaben aus dem *Liegenschaftskataster* auf maschinenlesbaren Datenträgern gespeichert erhalten (vgl. § 28 Abs. 1 Nr. 2 i. V. m. § 17 Abs. 7 Vermessungsgesetz). Mit Änderung der Liegenschaftskataster-Abgabeverordnung[127] wurde nun auch die Rechtsgrundlage für eine Abgabe der *Grundstückseigentümerdaten* auf maschinenlesbaren Datenträgern an die BWB geschaffen. Eine solche Datenübermittlung hat hinsichtlich der Privatkunden der BWB noch nicht stattgefunden. Eine Übermittlung von Eigentümerdaten aus dem Liegenschaftskataster wird erst notwendig, wenn die BWB sämtliche Grundstücke mit ihrer Kundendatei abgeglichen haben und daraufhin der Eigentümer eines Grundstücks ermittelt werden muss, für das bisher keine Abgaben erhoben wurden. Ebenfalls ergänzt wurde die Verordnung über die Verarbeitung personenbezogener Daten bei den Berliner Stadtreinigungsbetrieben, den Berliner Verkehrsbetrieben und den Berliner Wasserbetrieben[128], so dass damit auch die datenschutzrechtlichen Voraussetzungen für die weitere Verarbeitung der Grundstücksdaten durch die BWB geschaffen wurden. Hierzu zählt insbesondere die konkrete Berechnung des entsprechenden Entgelts für Schmutz- und Niederschlagswasser für die einzelnen Haushalte. Die getrennte Entgeltberechnung wurde zum 1. Januar 2000 eingeführt.

Verarbeitung von personenbezogenen Daten bei Heizkostenabrechnungen

Zur Überprüfung der vom Vermieter übersandten Heizkostenabrechnung - insbesondere der Verteilung der Gesamtkosten auf die einzelnen Wohneinheiten sowie der Berücksichtigung von Wohnungsleerstand – baten die Mieter eines Mietshauses um die Übersendung von Kopien der Gesamtabrechnung, aus der sich auch die Verbrauchsdaten zu den einzelnen Wohnungen und die darauf angerechneten Kosten ablesen lassen. Der Vermieter lehnte dies unter Hinweis auf den Datenschutz ab.

Dem Vermieter ist insoweit zuzustimmen, als hier datenschutzrechtliche Belange der *Mieter,* für deren Wohnungen die Verbrauchs- und Kostenangaben erbeten werden, berührt sind. Bei der Weitergabe dieser Daten an die auskunftbegehrenden Mieter handelt es sich um eine

127 GVBl. S. 506
128 GVBl. S. 586

Übermittlung von personenbezogenen Daten, die hier jedoch auf § 28 Abs. 2 Nr. 1 a) BDSG gestützt werden kann. Danach ist die Übermittlung zulässig, wenn sie zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Das berechtigte Interesse umfasst nicht nur ein rechtliches oder rechtlich geschütztes Interesse, sondern jeden – z. B. auch jeden akzeptablen wirtschaftlichen – Zweck. Das berechtigte Interesse der auskunftbegehrenden Mieter an der Datenübermittlung ergibt sich hier aus dem Mietvertragsverhältnis.

Erfolgt die Abrechnung der *Heizkosten* nicht nur pauschal (z. B. nach der Wohnungsgröße), sondern wird der individuelle Verbrauch als Grundlage für die Berechnung herangezogen, ist eine ordnungsgemäße Verbrauchserfassung nur anhand der einzelnen Abrechnungsbelege möglich. Wird auf den persönlichen Einzelverbrauch abgestellt, gehen unrichtig ermittelte Verbrauchswerte zu Lasten der übrigen Mitmieter. Insoweit hat der Nutzer/Mieter auch ein berechtigtes Interesse an den Heizungsabrechnungsdaten der Mitmieter. Nur in Kenntnis der (Verbrauchs-)Stricheinheiten der Mitmieter ist die Richtigkeit der in der individuellen Abrechnung angegebenen Gesamtheit aller verbrauchten Stricheinheiten zu überprüfen.

Damit kann jedoch nicht eine Offenlegung aller Daten der anderen Mietparteien durch den Vermieter gerechtfertigt werden. Zulässig ist nur das, was für die vollständige Kontrolle erforderlich ist. Eine Detailauflistung ist also nur dann zulässig, wenn es Anhaltspunkte für eine fehlerhafte Berechnung der Abrechnungsdaten gibt. Diese sind z. B. dann gegeben, wenn Verbrauchszahlen im Vergleich zu den Vorjahren erheblich differieren oder die Berücksichtigung von Wohnungsleerstand zweifelhaft ist. Da jeder einzelne Mieter ein Interesse an der Richtigkeit der Heizungsabrechnung hat, besteht insofern kein Grund zu der Annahme, dass die Betroffenen (Mitmieter) ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben.

Angabe der neuen Adresse beim Ausscheiden aus dem Mietvertrag

Beim Ausscheiden eines Mieters aus einem gemeinsamen Mietvertrag wird von den Betroffenen oft eine Verzichtserklärung verlangt. Diese ist gemeinsam, sowohl vom ausscheidenden als auch vom verbleibenden Mieter, zu unterzeichnen. Der Vordruck einer Wohnungsbaugesellschaft sah vor, dass der ausscheidende Mieter seine neue Adresse anzugeben hat. Eine Bürgerin hatte sich von ihrem gewalttätigen Partner (und Mitmieter) getrennt und befürchtete, dass dieser über die Angaben in der Verzichtserklärung ihre neue Adresse in Erfahrung bringen könnte.

Die Erhebung und Verarbeitung der neuen Adresse des ausscheidenden *Mieters* ist unzulässig.

Insbesondere kommt hier der Verweis auf § 28 Abs. 1 Nr. 1 BDSG, wonach es zulässig ist, personenbezogene Daten für die Erfüllung eigener Geschäftszwecke im Rahmen eines Vertragsverhältnisses mit dem Betroffenen zu speichern, nicht in Betracht. Die Datenverarbeitung erfolgt hier anlässlich der Auflösung eines bestehenden Vertragsverhältnisses. Hierfür ist die Speicherung der neuen Adresse des bisherigen Vertragspartners jedoch nicht erforderlich. Zur Geltendmachung eventuell bestehender Forderungen kann eine Melderegisterauskunft eingeholt werden. Die regelmäßige Speicherung der neuen Adressen aller ehemaligen Vertragspartner ist dagegen eine unzulässige Datenspeicherung auf Vorrat.

Die Wohnungsbaugesellschaft ist unserer Empfehlung gefolgt und wird in Zukunft auf die Erhebung und Speicherung der neuen Adresse des ausscheidenden Mieters verzichten. Der Vordruck der Verzichtserklärung wurde überarbeitet und enthält keine derartigen Textfelder mehr.

Benennung von WBS-Inhabern ohne dringenden Wohnbedarf an private Vermieter

Angesichts der steigenden Anzahl von zur Vermietung freistehendem Wohnraum hatten einzelne Vermieter die Senatsverwaltung für Bauen, Wohnen und Verkehr darum gebeten, geeignete Wohnungssuchende (WBS-Inhaber) benannt zu bekommen, auch wenn die Wohnungen nicht dem Besetzungsrecht Berlins unterliegen. Daraufhin hat die Senatsverwaltung für Bauen, Wohnen und Verkehr das Benennungsverfahren – als zusätzliches Serviceangebot – insofern erweitert, dass bei Bedarf auch WBS-Inhaber ohne dringenden Wohnbedarf den Vermietern benannt werden.

Während die *WBS*-Antragsteller mit dringendem Wohnungsbedarf im Rahmen der behördlichen Mithilfe bei der *Wohnraumbeschaffung* in den entsprechenden Formularen über die Bekanntgabe ihrer Daten (Name, Adresse, Anzahl der mit einziehenden Angehörigen, WBS-Antragsnummer) an den Vermieter informiert wurden und dazu ihre Einwilligung erteilten, war dies für die Betroffenen *ohne* dringenden Wohnbedarf nicht der Fall. Wir haben empfohlen, den Vordruck entsprechend zu ergänzen, um auch diesen Personenkreis über die Datenübermittlung an die Vermieter zu informieren. Die Senatsverwaltung ist dieser Empfehlung gefolgt. In der Neufassung des Vordruckes kann der Antragsteller zukünftig – unabhängig davon, ob die Kriterien eines dringenden Wohnbedarfs vorliegen oder nicht – um die behördliche Mithilfe bei der Wohnraumbeschaffung bitten. Eine Übermittlung von personenbezogenen Daten des Antragstellers (Name, Anzahl der mit ein-

ziehenden Angehörigen und WBS-Antragsnummer) an den Vermieter erfolgt nur noch in den Fällen, in denen der Betroffene in diese Übermittlung eingewilligt hat. Eine Differenzierung bei der Aufklärung über die Übermittlung danach, ob ein dringender Wohnbedarf besteht oder dies nicht der Fall ist, ist somit nicht mehr gegeben.

Nutzungsentgelte für Datschengrundstücke

Das Land Berlin tritt in verschiedenen Bereichen als Verpächter von Grundstücken auf. In diesem Zusammenhang wurden wir gefragt, ob es zulässig sei, den Nutzern von Datschengrundstücken auf dem Gebiet der ehemaligen DDR in Entgelterhöhungsschreiben – zur Ermittlung der ortsüblichen Entgelte – die Adressen von vergleichbaren Grundstücken zu übermitteln.

Mit der *Nutzentgeltverordnung* (NutzEV) vom 22. Juli 1993[129] hat der Gesetzgeber bezweckt, die Nutzungsentgelte für Erholungsgrundstücke (Datschen) auf dem Gebiet der ehemaligen DDR, die regelmäßig sehr niedrig waren, schrittweise und sozialverträglich auf das ortsübliche Entgelt für vergleichbar genutzte Grundstücke anzuheben. Nachdem 1996 in weiten Bereichen bereits das ortsübliche Niveau bei den Entgelten erreicht war, wurde mit der Änderung der NutzEV im Jahr 1997[130] in § 6 Abs. 1 eine Erläuterungspflicht für Erhöhungsverlangen eingeführt. Ziel dieser Regelung ist, dass sich der Grundstückseigentümer vor einer weiteren Erhöhung über die ortsüblichen Entgelte informiert[131]. Bezüglich der Erläuterungspflicht – und der darin enthaltenen Daten zu Vergleichsgrundstücken – werden an die Grundstückseigentümer keine überzogenen Erwartungen gestellt. Es ist ausreichend, wenn in der Erhöhungserklärung Hinweise und Angaben gemacht werden, die es dem Nutzer ermöglichen, die Berechtigung der Erhöhung zu überprüfen.

Zur Ermittlung der ortsüblichen Nutzungsentgelte besteht nach § 7 Abs. 1 NutzEV ein Auskunftsanspruch gegenüber dem zuständigen *Gutachterausschuss.* Dieser hat dem Antragsteller – in anonymisierter Form – Auskunft über die in seinem Geschäftsbereich vereinbarten Entgelte unter Angabe der Gemarkung, in der die Grundstücke liegen, zu erteilen. Liegen dem Gutachterausschuss keine Erkenntnisse über vergleichbare Grundstücke mit frei vereinbarten Entgelten vor, ist – neben dem Vergleichsverfahren – subsidiär das *Bodenwertverzinsungsverfahren* zur Ermittlung des Entgeltes zugelassen (§ 3 Abs. 3 NutzEV). Die Praxis der Gutachterausschüsse hat gezeigt, dass das Bodenwertverzinsungsverfahren – als eine vom Gesetzgeber hilfsweise zugelassene Methode – zur Ermittlung des ortsüblichen Entgeltes geeignet ist.

---

129 BGBl. I S. 1339
130 BGBl. I S. 1920
131 BR-Drs. 1/97, S. 9

Dagegen ist eine Rechtsvorschrift, die es dem Eigentümer/Verpächter erlaubt, personenbezogene Daten im Zusammenhang mit Vergleichsgrundstücken an Dritte zu übermitteln, nicht ersichtlich. Auch in der NutzEV ist eine derartige Übermittlungsbefugnis nicht geregelt. Die Übermittlung von Adressen zur Ermittlung der ortsüblichen Entgelte an die Nutzer der Datschengrundstücke ist daher nur mit Einwilligung der Eigentümer oder Nutzer der Vergleichsgrundstücke erlaubt.

Vergleichswohnungen bei Mieterhöhungen

Zu klären war, welche Angaben über Dritte in Mieterhöhungsschreiben mitgeteilt werden dürfen. Ein Bürger beschwerte sich darüber, dass er in der Anlage zu einem Mieterhöhungsschreiben von seinem Vermieter eine Liste mit Vergleichswohnungen erhalten hat, in der unter anderem auch personenbezogene Daten (Name, Vorname) der Mieter dieser Wohnungen angegeben waren.

Nach § 2 Abs. 1 Nr. 2 *Miethöhegesetz* (MHG) muss der Vermieter in seinem Mieterhöhungsverlangen begründet darlegen, dass die verlangte erhöhte Miete die ortsübliche Miete nicht übersteigt.

Mit dem Hinweis auf die ortsübliche *Vergleichsmiete* hat der Gesetzgeber seine Absicht zum Ausdruck gebracht, Mieterhöhungen in bestehenden Mietverhältnissen auf die ortsüblichen Entgelte für vergleichbare Wohnungen in der Gemeinde zu begrenzen. Er hat durch das Vergleichsmietensystem einen Ausgleich geschaffen zwischen dem Interesse des Vermieters, eine möglichst hohe Miete erzielen zu können, und dem Interesse des Mieters, den einmal vereinbarten Mietzins möglichst lange unverändert zahlen zu müssen. Der unbestimmte Rechtsbegriff der „ortsüblichen Vergleichsmiete“ umfasst die üblichen Entgelte, die in der Gemeinde für nicht preisgebundenen Wohnraum vergleichbarer Art, Größe, Ausstattung, Beschaffenheit und Lage in den letzten vier Jahren vereinbart oder geändert worden sind. Gebildet wird die ortsübliche Vergleichsmiete aus dem Durchschnitt aller Mieten für vergleichbaren Wohnraum, die zum Zeitpunkt des Zugangs des Erhöhungsverlangens gezahlt werden.

Dem Mieterhöhungsverlangen des Vermieters muss stets eine Begründung zugrunde liegen. Der Zweck des Begründungserfordernisses liegt darin, dem Mieter die Möglichkeit der Information und der Nachprüfbarkeit zu geben, damit er aufgrund der ihm mitgeteilten Daten entscheiden kann, ob er dem Mieterhöhungsverlangen zustimmen will oder nicht.

Der Gesetzgeber hat in § 2 Abs. 2 MHG drei Begründungsmöglichkeiten für ein Mieterhöhungsverlangen für zulässig erklärt. Zulässig sind die Bezugnahme auf einen Mietspiegel (§ 2 Abs. 2 Satz 2 MHG), die Erstellung eines Sachverständigengutachtens (§ 2 Abs. 2 Satz 3 MHG) und die Angabe von einzelnen Vergleichswohnungen (§ 2

Abs. 2 Satz 4 MHG). Diese Aufzählung ist exemplarisch und nicht abschließend. Zugelassen sind alle Begründungsmöglichkeiten, wenn sie nur geeignet sind, dem Mieter die für die Entschließung zur Zustimmung erforderliche Information zu geben.

Das Gesetz erwähnt den *Mietspiegel* an erster Stelle, weil die Darlegung der ortsüblichen Vergleichsmiete unter Angabe von einzelnen Vergleichswohnungen alle Beteiligten vor beträchtliche Schwierigkeiten stellt. Diese Form der Begründung des Erhöhungsverlangens sollte nach den Vorstellungen des Gesetzgebers die Ausnahme bleiben, da ein statistisch erstellter Mietspiegel die ortsübliche Vergleichsmiete mit einer sehr viel höheren Wahrscheinlichkeit wiedergibt als drei vom Vermieter willkürlich ausgewählte einzelne Vergleichswohnungen.

Das Bundesverfassungsgericht hat die Bedeutung von Mietspiegeln mehrfach ausdrücklich betont[132]. Nach Ansicht des Gerichts liegt die Verwendung von Mietspiegeln im gerichtlichen Erkenntnisverfahren auch im Interesse der Vermieter. Sie garantiert nicht nur eine schnelle Entscheidung, sie erleichtert dem Vermieter zugleich in ganz erheblichem Maße die ihm obliegende prozessuale Darlegungslast.

Dagegen ist die Angabe von drei einzelnen *Vergleichswohnungen* zur Begründung des Mieterhöhungsverlangens problematisch. Dabei ist zwischen der Frage, wie eine Wohnung objektiv beschaffen sein muss, um als Vergleichswohnung herangezogen werden zu können, und der Frage, welche Informationen dem Mieter über die Vergleichswohnung zu übermitteln sind, zu unterscheiden. Der Wortlaut des § 2 Abs. 2 Satz 4 MHG ist diesbezüglich wenig ergiebig. Dort ist nur von einem „Hinweis“ sowie einer „Benennung“ der Wohnung die Rede. Diese Formulierungen des Gesetzgebers lassen eine sehr enge Auslegung zu, bei der dem Mieter nur sehr wenige Angaben über die Vergleichswohnung zu machen sind, aber auch eine sehr weite Auslegung, wonach dem Mieter im Erhöhungsverlangen sehr detaillierte Informationen mitzuteilen sind.

Die Rechtsprechung fordert, dass der Vermieter die Vergleichswohnungen so konkret bezeichnen muss, dass sie für den Mieter zweifelsfrei zu identifizieren sind. Dazu sind in jedem Fall Angaben zur postalischen Anschrift (Ort, Straße, Hausnummer) erforderlich. Sind unter der Anschrift mehrere Wohnungen (z. B. in einem Mehrparteienmietshaus) zu finden, hat der Vermieter weitere Angaben zur Identifizierung des Objekts (z. B. Wohnungsnummer, Geschosszahl, linker oder rechter Seitenflügel usw.) zu machen. Dagegen sind Angaben zum Namen und Vornamen der Mieter der Vergleichswohnungen nur in Ausnahmefällen erforderlich, um das Objekt zu identifizieren.

---

132 Beschluss v. 3. 4. 1990, Az.: 1 BvR 268/98, NJW 1992, S. 1377

In jedem Fall handelt es sich bei den vorstehenden Angaben um personenbezogene Daten des Mieters. Durch die Anschrift und die weiteren Angaben zur Lage der Wohnung ist er bestimmbar, durch die genaue Beschreibung der Ausstattungsmerkmale kann auf seine Lebensumstände, insbesondere seine Wohnverhältnisse geschlossen werden.

Dem berechtigten Interesse des Vermieters, das Mieterhöhungsverfahren durchzuführen, steht das schutzwürdige Interesse der Mieter der Vergleichswohnungen an der Geheimhaltung der Daten entgegen (vgl. § 28 Abs. 1 Nr. 2 BDSG).

Die Übermittlung der Wohnungsdaten ist deshalb nur mit Einwilligung der Mieter in den Vergleichswohnungen zulässig. Die Einwilligung ist nach § 4 Abs. 1 BDSG schriftlich vom Betroffenen einzuholen. Dieser ist über den vorgesehenen Verwendungszweck der Daten und darüber zu informieren, dass die Einwilligung widerruflich ist.

Übermittlung von Mieterdaten an das Sozialamt bei Mietzinsrückständen

Aufgrund von Mietzahlungsrückständen sah sich eine Wohnungsbaugesellschaft dazu veranlasst, gegen den Mieter eine fristlose Kündigung des Mietvertrages auszusprechen. Parallel dazu wurde dem zuständigen Sozialamt – zur Vermeidung einer Obdachlosigkeit des Mieters – eine Kopie des Kündigungsschreibens übersandt. Der Mieter – der regelmäßig und fristgerecht seinen Mietzins überwiesen hatte – war über diesen Vorgang empört. Der mit der Überweisung beauftragten Bank war bei der Datenerfassung der Kontonummer des Zahlungsempfängers (Vermieter) ein Fehler unterlaufen. Dies hatte zur Folge, dass die Zahlungseingänge auf einem anderen Mieterkonto verbucht wurden.

Gestützt wurde die Maßnahme von der *Wohnungsbaugesellschaft* – unter Bezugnahme auf Empfehlungen des Berliner Datenschutzbeauftragten aus dem Jahr 1992 – auf die §§ 20 und 69 SGB X.

Die datenschutzrechtliche Beurteilung aus dem Jahr 1992 erfolgte zu der Fragestellung, ob Sozialämter – um eine drohende *Obdachlosigkeit* zu verhindern – an den Vermieter herantreten dürfen und ob dieser daraufhin Daten des Mieters übermitteln darf. Gegenstand der damaligen Überlegungen war eine klar definierte soziale Randgruppe, der unmittelbar die Obdachlosigkeit droht, die aber zugleich als Problemklientel ihrer Mitwirkungspflicht i.S.d. Sozialgesetzbuches (§ 60 SGB I) offensichtlich nicht genügen kann oder will.

Für diese Fälle sieht Nr. IV/1 der Anordnung über *Mitteilungen in Zivilsachen* (MiZi) eine Übermittlungspflicht vor. Danach hat das Zivilgericht den Umstand des Einganges einer Klage, mit der die Räumung von Wohnraum im Falle der Kündigung des Mietverhältnisses wegen Zahlungsverzuges des Mieters nach § 554 BGB verlangt wird, dem

Sozialamt mitzuteilen (vgl. Nr. IV/1 Abs. 5 MiZi). Gleichzeitig ist der Betroffene über den Inhalt und den Empfänger der Mitteilung zu unterrichten (Nr. IV/1 Abs. 6 MiZi). Erhält das Sozialamt die Mitteilung vom Gericht, kann es – um die Wohnung zu erhalten und eine Obdachlosigkeit zu vermeiden – an den Vermieter herantreten und diesem anbieten, rückständige Mietzahlungen zu übernehmen. Der Vermieter kann dieses Angebot annehmen und dabei offenbaren, dass die Betroffenen tatsächlich in einem Mietverhältnis zu ihm stehen bzw. in welcher Höhe Mietrückstände bestehen.

Davon zu unterscheiden sind – wie im vorliegenden Fall – „Spontanübermittlungen" an das Sozialamt durch den Vermieter, die nur mit Einwilligung des Mieters zulässig sind. In keinem Fall dürfen diese hinter dem Rücken des Mieters erfolgen. Eine gesetzliche Befugnis ist nicht ersichtlich. Insbesondere bieten § 20 SGB X – Untersuchungsgrundsatz – und § 69 SGB X – Übermittlung für die Erfüllung sozialer Aufgaben – keine Rechtsgrundlage für eine derartige Datenübermittlung durch den Vermieter.

Nicht zulässig sind auch Regelanfragen, in denen das Sozialamt an den Vermieter herantritt und diesen auffordert mitzuteilen, ob und wie viele Kündigungen wegen Zahlungsverzuges nach § 554 BGB in einem bestimmten Zeitraum ausgesprochen wurden. Von dieser Maßnahme würden – ohne Ausnahme – alle Mieter erfasst, bei denen ein Mietzinsrückstand (aus welchem Grund auch immer) besteht. Infolge der Anfragen würden beim Sozialamt – anlassunabhängig – über eine Vielzahl von Betroffenen Daten verarbeitet, ohne dass die Voraussetzungen des BSHG vorliegen.

4.4.5 Tier und Pflanze

Datenschutz für Hundehalter?

„Der tut nix!", ist ein oft von Hundehaltern gehörter Spruch. Leider bewahrheitet sich diese Ankündigung nicht immer. Angriffe und Bisse durch aggressive Hunde erschrecken immer wieder die Öffentlichkeit. Um diese von gefährlichen Hunden ausgehenden Risiken besser zu bekämpfen, wurde die Verordnung über das Halten von Hunden in Berlin vom 5. November 1998 (HundeVO Bln)[133] *erlassen.*

Wenn sich ein Hund als gefährlich erwiesen hat, weil er z. B. wiederholt in Gefahr drohender Weise Menschen angegriffen hat, sind neben den erforderlichen Auflagen (insbesondere Leinen- oder Maulkorbzwang) oder Maßnahmen, die bis zur Sicherstellung und/oder Tötung des Hundes führen können, die Sachkunde und *Zuverlässigkeit des Hundehalters* zu überprüfen. Die Diskussion, ob – wie in Brandenburg –

[133] GVBl. S. 326

eine Liste mit Rassen der als gefährlich einzustufenden Hunde der bessere Weg ist, ist keine Sache des Datenschutzes, wohl aber die Frage, welche Daten von Haltern unter welchen Voraussetzungen und wie lange bei den Veterinärämtern gespeichert werden dürfen. Weiterhin ist festzulegen, bei Vorliegen welcher Voraussetzungen die Zuverlässigkeitsüberprüfung der Halter durchgeführt werden darf und welche Überprüfungen im Einzelnen erfolgen. Dies alles lässt die Verordnung offen. Die Senatsverwaltung für Gesundheit und Soziales ist unserer Anregung – auch nach einer Besprechung im Unterausschuss „Datenschutz" – nicht gefolgt, so dass letztlich das Abgeordnetenhaus hierüber entscheiden musste[134]. Es hat den Senat aufgefordert, in die HundeVO Bln auch die von uns vorgeschlagenen Veränderungen aufzunehmen[135].

Nach der Entscheidung des Bundesverwaltungsgerichtes am 19. Januar 2000 zu der Zulässigkeit einer höheren Hundesteuer für bestimmte *„Kampfhund-Rassen"* ist die Diskussion um die Neuorientierung der Hundeverordnung erneut entbrannt. Die höhere Besteuerung hätte aus der Sicht des Datenschutzes jedenfalls den Vorteil, dass das Sammeln von Informationen über die Hundehalter entfiele, jedenfalls solange der Hund nicht auffällig geworden ist. Bei dem darüber hinaus zum Teil geforderten generellen Verbot des Haltens und des Erwerbes bestimmter Hunderassen (mit Tötungsverfügung bei Zuwiderhandlung?) würde zwar die Zuverlässigkeitsüberprüfung der Halter entfallen; ob eine derartige Regelung aber noch verhältnismäßig ist, ist fraglich. Unabhängig davon, ob eine Rasse-Liste (mit Genehmigungsvorbehalt und Zuverlässigkeitsprüfung des Halters) eingeführt wird oder ob eine Zuverlässigkeitsüberprüfung nach konkreten Bissvorfällen – unabhängig von der Hunderasse – erfolgt: In jedem Fall müssen klare Datenverarbeitungsregelungen aufgenommen werden. Die Senatsverwaltung für Gesundheit und Soziales hat inzwischen zugesagt, in dem nunmehr beabsichtigten Gesetz über das Halten und Führen von Hunden die Datenerhebungsbefugnisse zu konkretisieren und klarzustellen, dass im Rahmen der Zuverlässigkeitsüberprüfung ein Führungszeugnis angefordert wird. Ferner wird geprüft, ob konkrete Löschungsfristen für die gespeicherten Halterdaten aufgenommen werden.

Datenbank für Tierschutzfälle

Die Tierärztliche Vereinigung für den Tierschutz e. V. (TVT) plant in Zusammenarbeit mit dem Tierschutzzentrum der tierärztlichen Hochschule Hannover die Errichtung einer Datenbank für Tierschutzfälle. Zur Erfassung der jeweiligen Umstände der Einzelfälle wurde von der TVT dazu ein Fragebogen entwickelt. Dieser wurde den Tierschutzreferenten und Tierschutzbeauftragten der Länder mit der Bitte übersandt,

134 Beschluss des Abgeordnetenhauses v. 25. 3. 1999

135 vgl. Beschlussempfehlung des Ausschusses für Gesundheit, Soziales und Migration v. 18. 3. 1999 über Nachbesserung der Berliner Hundeverordnung, Abghs.-Drs. 13/3587

auf die ihnen nachgeordneten Behörden dahingehend einzuwirken, die dort bearbeiteten Einzelfälle auf dem Fragebogen zu dokumentieren und der TVT zu melden.

Das Verfahren stößt auf erhebliche datenschutzrechtliche Bedenken. Der Fragebogen enthält Angaben (z. B. Aktenzeichen, ausstellende Behörde, getroffene Maßnahmen usw.), über die eine Person, gegen die ein *Tierschutzverfahren* geführt wurde, bestimmbar ist. Es handelt sich somit um die Erhebung von personenbezogenen Daten und deren Übermittlung an die TVT. Eine Rechtsvorschrift, auf die eine derartige Verarbeitung der personenbezogenen Daten gestützt werden könnte, ist nicht ersichtlich.

Die Senatsverwaltung für Gesundheit und Soziales teilte unsere Bedenken. Die für den Vollzug des Tierschutzrechtes zuständigen Veterinär- und Lebensmittelaufsichtsämter von Berlin wurden dahingehend informiert, keine Informationen an die genannten Einrichtungen zu übermitteln.

Selbstauskunft bei Tiervermittlung

Zur Vermittlung von heimatlosen Tieren an zukünftige Tierhalter verwendete das Tierheim Lankwitz einen Fragebogen „Selbstauskunft", mit dem beim Interessenten umfangreiche Daten über seine Person und seinen Ehepartner bzw. Lebensgefährten erhoben und verarbeitet wurden.

Unbestritten ist, dass das *Tierheim* berechtigt ist, die personenbezogenen Daten der zukünftigen *Tierhalter* zu erheben, die es benötigt, um eine sachgerechte Tiervermittlung durchzuführen. Dies gilt unabhängig davon, ob die Daten in der Selbstauskunft Bestandteil des Überlassungsvertrages sind oder ob diese im Rahmen der Anbahnung eines zukünftigen Vertragsverhältnisses in einem Bewerbungsverfahren erhoben werden.

Angaben zu Geburtsort, Staatsangehörigkeit, Personalausweis- oder Reisepassnummer des Interessenten sind jedoch weder erforderlich, um die Identität des Interessenten festzustellen oder eine Verwechslung mit Dritten auszuschließen, noch um bei den Meldestellen eine Auskunft über die gegenwärtige Anschrift zu erhalten. Auch für die Einleitung gerichtlicher Maßnahmen (Erstattung einer Strafanzeige, Klageerhebung usw.) werden diese Daten nicht benötigt. Andere Gründe, warum diese Angaben für den Abschluss eines Tierüberlassungsvertrages erforderlich sein sollten, sind nicht ersichtlich. Die Erhebung und Speicherung dieser Daten ist daher unzulässig.

Angaben zum Vermieter/Untermieter sind für das Vertragsverhältnis ebenfalls nicht erforderlich. Soweit diese Angaben etwa dazu genutzt werden sollen, Erkundigungen über den Tierinteressenten einzuholen,

ist darauf hinzuweisen, dass eine derartige Datenerhebung hinter dem Rücken des Betroffenen grundsätzlich gegen Treu und Glauben verstößt und daher unzulässig ist (vgl. § 28 Abs. 1 Satz 2 BDSG).

Angaben zur Wohndauer („Seit wann wohnen Sie dort?/Wohnen Sie auch in den nächsten 8 Wochen dort?“) sind nicht geeignet, falsche Angaben zur Person oder zum Wohnort aufzudecken oder zu verhindern. Soweit sie dazu dienen sollen, eine gewisse „Sesshaftigkeit“ des Interessenten festzustellen, ist nicht erkennbar, warum dies für den Vertragszweck von Bedeutung sein soll.

Soweit Angaben zur Person des Ehepartners/Lebensgefährten oder die Kontaktadresse eines Bekannten erfragt werden, handelt es sich um die Daten von Dritten, die grundsätzlich beim Betroffenen selbst zu erheben sind. Darüber hinaus ist die Erforderlichkeit zur Verarbeitung dieser Daten nicht ersichtlich. Die Angaben über den Tierinteressenten genügen, um eventuell Nachkontrollen durchführen zu können. Um die Betreuung des Tieres auch während der (z. B. beruflichen) Abwesenheit des Tierhalters sicherzustellen, kann eine entsprechende Verpflichtung vertraglich festgelegt werden. Angaben dazu, welche Personen (Angaben über Dritte) dieser Verpflichtung – im Auftrag des Tierhalters – nachkommen werden, sind dagegen nicht erforderlich.

Das Tierheim ist unseren Empfehlungen für eine datenschutzgerechte Gestaltung des Formulars „Selbstauskunft“ gefolgt. Die geänderte Fassung des Vordruckes, in dem die nicht erforderlichen Daten nicht mehr erfasst werden, schafft einen Ausgleich zwischen dem Interesse an einer sachgerechten, am Wohl des Tieres orientierten Vermittlung und dem Recht auf informationelle Selbstbestimmung der zukünftigen Tierhalter.

Sachkunde bei Pflanzenschutzmitteln

Eine Gartenbaufirma beschwerte sich bei uns darüber, dass das Pflanzenschutzamt Berlin bzw. die Senatsverwaltung für Stadtentwicklung, Umweltschutz und Technologie zum Nachweis der Sachkunde der Beschäftigten beim Umgang mit Pflanzenschutzmitteln die Vorlage von Prüfungszeugnissen oder Ausbildungsnachweisen verlangte. Die Firma sah darin einen Verstoß gegen datenschutzrechtliche Bestimmungen, da diese Unterlagen Angaben – z. B. Leistungsbewertungen, Berufsabschlüsse mit Einzelnoten – enthalten, die ihr von den Beschäftigten vertraulich überlassen wurden.

Das Ansinnen, einen Sachkundenachweis der Beschäftigten zu verlangen, ist kein Verstoß gegen datenschutzrechtliche Bestimmungen. Die Erhebung von personenbezogenen Daten der Beschäftigten kann auf §§ 9 und 10 *Pflanzenschutzgesetz* (PflSchG) i.V.m. § 2 der Verordnung über die Anzeige der Anwendung von Pflanzenschutzmitteln und über das Prüfungsverfahren für den Nachweis der pflanzenschutzlichen Sachkunde (AnzPrüfOPflSch) gestützt werden.

4.5.1

Nach § 9 PflSchG ist der gewerbliche Umgang mit *Pflanzenschutzmitteln* der zuständigen Behörde vor Aufnahme der Tätigkeit anzuzeigen. Die Anzeige muss Name und Anschrift des Betriebes, des Betriebsinhabers und der Personen, die Pflanzenschutzmittel anwenden, sowie einen Sachkundenachweis für diese Personen enthalten (§ 25 AnzPrüfOPflSch). Der *Sachkundenachweis* kann z. B. durch Prüfungszeugnisse oder Ausbildungsnachweise erbracht werden.

Das Zeugnis über die bestandene Prüfung enthält nach § 9 Abs. 2 AnzPrüfOPflSch die Bezeichnung der Prüfung, die Personalien des Prüfungsteilnehmers, Ort und Datum der Prüfung und die Feststellung über das Bestehen der Prüfung. Weitere Angaben zu Leistungsmerkmalen, -bewertungen, -beurteilungen, Berufsabschlüssen und Einzelbenotungen werden nicht verlangt. Daraus wird ersichtlich, dass diese zusätzlichen Angaben für den Nachweis der Sachkunde nicht erforderlich sind.

Der Sachkundenachweis kann auch durch Vorlage anderer Zeugnisse, z. B. Ausbildungsnachweise, erbracht werden. Soweit diese Angaben (z. B. Benotungen) enthalten, die über den Katalog der in § 9 Abs. 2 AnzPrüfOPflSch genannten Daten hinausgehen, können diese unkenntlich gemacht werden. Nach dem Willen des Gesetzgebers ist jedoch der allgemeine Hinweis, eine einschlägige Berufsausbildung mit den vorgesehenen Ausbildungsgraden abgeschlossen zu haben, allein für den Nachweis der Sachkunde nicht ausreichend.

4.5 Wissen und Bildung

4.5.1 Wissenschaft und Forschung

Ende 1997 gab die Kommission „Selbstkontrolle der Wissenschaft" der *Deutschen Forschungsgemeinschaft* (DFG) Empfehlungen zur „Sicherung guter wissenschaftlicher Praxis" heraus. Hintergrund war die Veröffentlichung von Forschungsergebnissen aufgrund fingierter Daten. Im Jahresbericht 1998 verwiesen wir auf eine Initiative der Universität Freiburg[136]. Die Freie Universität Berlin erarbeitete, wie schon zuvor die Humboldt-Universität, einen auf den Empfehlungen der DFG aufbauenden *Ehrenkodex* zur Sicherung guter wissenschaftlicher Praxis, der Mitte des Jahres dem Akademischen Senat vorlag.

Zur Sicherung der Überprüfbarkeit durch unabhängige wissenschaftliche Instanzen bei Zweifeln an der Redlichkeit der angewandten wissenschaftlichen Methoden wird eine Aufbewahrung von *Primärdaten* für zehn Jahre vorgesehen. Diese Aufbewahrungsfrist ist zwar aus der Sicht der Wissenschaftler nachvollziehbar, jedoch datenschutzrechtlich nicht unproblematisch. Im Rahmen von Einwilligungserklärungen

136 JB 1998, 4.5.1

muss verbindlich dargelegt werden, in welchen Stufen die Einzelangaben anonymisiert werden. Das Berliner Datenschutzgesetz verlangt eine Löschung der Merkmale, mit denen ein Personenbezug hergestellt werden kann, sobald der Forschungszweck erreicht ist (§ 30 Abs. 2). Hilfsmerkmale, die auf die Person hinweisen oder mit denen ein Personenbezug herstellbar ist, sind damit nach Abschluss des Forschungsvorhabens zu löschen.

Häufig ergibt sich auch aus der Kombination der „Erhebungsmerkmale“ selbst ein großes Potenzial zur Wiederherstellung des Personenbezuges. Auch Primärdaten ohne Hilfsmerkmale sind damit häufig als nicht hinreichend anonymisiert anzusehen. Oft wird den Betroffenen mit der Information zu ihrer Einwilligungserklärung zugesichert, dass die Daten „nur im Rahmen dieses Forschungsvorhabens“ verwendet werden. Damit ist eine Überprüfung der Forschungsergebnisse rechtlich nicht abgesichert. Die Überprüfung des Forschungsprojektes ist eine Zweckänderung, die einer gesonderten Einwilligung bedarf. In der Einwilligungserklärung muss auf die Verpflichtung der Wissenschaftler zur Einhaltung des jeweiligen Ehrenkodex ihrer Hochschule und die Aufbewahrung der Daten zur Überprüfung verwiesen werden. Es ist allerdings fraglich, ob die Betroffenen einer zehnjährigen personenbezogenen Aufbewahrung ihrer Unterlagen zustimmen werden.

Bei der anstehenden Novellierung des Berliner Datenschutzgesetzes im Zusammenhang mit der EU-Richtlinie sollte geprüft werden, ob eine der Anonymisierung gleichzusetzende organisatorische Möglichkeit statt einer Löschung vorgesehen werden kann. Neben oder verbunden mit einer Pseudonymisierung könnte ein *Datentreuhänderverfahren* genutzt werden. Der Datentreuhänder könnte dann als Adressmittler versuchen, mit den Betroffenen in Kontakt zu treten, ohne dass ihm selbst die sensiblen Erhebungsdaten vorliegen, da er lediglich die Hilfsmerkmale sicher verwahrt. Ergänzend könnte auch in das Berliner Hochschulgesetz eine Regelung aufgenommen werden, die den Hochschulen die Verpflichtung zur Schaffung von Ehrenkodizes auferlegt und somit eine Übermittlung von Forschungsdaten durch die Forscher an eine mit Aufsichts- und Kontrollbefugnissen ausgestattete Instanz der Hochschule legitimieren würde.

Datenschutzgerechte Forschung

Immer wieder bringen Forscher vor, der Datenschutz behindere ihre Arbeit. Die Beratungen, die wir in großer Zahl durchführen, beweisen das Gegenteil: Forschungsprojekte können immer so gestaltet werden, dass Wissenschaftsfreiheit und informationelle Selbstbestimmung in Einklang gebracht werden können. Wie jedes Jahr hier eine Auswahl der Projekte, die wir beraten haben.

Von den Forschern befragt wurden

- jugendliche Aussiedler zur Integration
- Frauen zu oralen Kontrazeptiva
- Diabeteskranke nach ihrer Betreuung durch die Krankenkasse
- Lehrer zur Gewalt an der Schule
- Schüler über ihre Kopfschmerzen
- Zeitzeugen zum Mauerbau an der Bernauer Straße
- Mitarbeiter zur Gleichstellung von Frauen
- Halter von Hunden und Opfer von Bissverletzungen.

Akteneinsicht wollten Forscher nehmen in Unterlagen über

- jüdische Rechtsanwälte nach 1933
- DDR-Kinderheime
- rechtsextreme Straftäter
- Berufsverläufe in der Medizin
- Zahnpflege von Kindern in schulzahnärztlichen Akten.

Eines der größten Projekte, die die Datenschutzbeauftragten gemeinsam beraten haben, ist eine internationale Schulvergleichsstudie der OECD (PISA).

Unzulässige Veröffentlichungen über Hochschulaccounts

Das Internet wurde – nach militärischen Anfängen – an amerikanischen Hochschulen entwickelt und hat seinen weltweiten Siegeszug als globales Forschungsnetz begonnen. Es wurde lange als Bereich der unbeschränkten Meinungsfreiheit betrachtet, kein Wunder, dass die Möglichkeiten von Anfang an auch zur Begehung von Straftaten oder zum Verstoß gegen Datenschutzbestimmungen genutzt wurden. Fraglich ist, welche Verantwortung die Hochschulen selbst dabei tragen.

Hochschulen als Anbieter von *Tele- und Mediendiensten* sind im Internet bei rechtswidrigen Veröffentlichungen für eigene Inhalte verantwortlich (§ 5 Teledienstegesetz; § 5 Mediendienste-Staatsvertrag). Diese Verantwortlichkeit besteht sowohl für das Angebot der *Hochschule* als Ganzes als auch für Angebote von Teilkörperschaften oder einzelnen Mitgliedern. Die Universität und ihre Teilkörperschaften unterliegen den Regelungen des Berliner Hochschulgesetzes und des Berliner Datenschutzgesetzes. Übermittlungen und damit auch die Veröffentlichungen personenbezogener Daten im Internet sind nur zulässig, wenn eine Rechtsvorschrift dieses erlaubt oder der Betroffene eingewilligt hat. Bestehen Zweifel an der Zulässigkeit der Veröffentlichung, ist

die Veröffentlichung bis zur Klärung der Angelegenheit zu sperren. Dies gilt auch, wenn Mitglieder oder externe Nutzer über ihre Accounts an der Hochschule private Veröffentlichungen vornehmen. Wir können den Hochschulen nur dringend empfehlen, von ihrer Satzungsbefugnis nach § 6 Berliner Hochschulgesetz Gebrauch zu machen und Ordnungen für die Nutzer sowie auch Regelungsmechanismen bei Verstößen gegen die Satzung bzw. andere Rechtsvorschriften festzuschreiben.

4.5.2 Schule

Neues Schulgesetz für Berlin

Es wurde ein Diskussionsentwurf für ein neues *Schulgesetz* vorgelegt, der die Zusammenführung von *Schulverfassungsgesetz* und Schulgesetz vorsieht. Im Interesse normenklarer Regelungen begrüßen wir dies, ebenso wie die vorgesehene Überführung vieler Verwaltungsvorschriften mit erheblichen Außenwirkungen in Rechtsverordnungen.

Einzelne der in dem Gesetzentwurf enthaltenen Regelungen sind datenschutzrechtlich bedenklich. In einer breiten Öffentlichkeit wurde die erweiterte Selbstverwaltung und Eigenverantwortung, die dieser Entwurf vorsah, diskutiert. Insbesondere die Vorschläge zur *Qualitätssicherung* und *Evaluation* ließen die datenschutzrechtlichen Aspekte zunächst außer Acht. Gerade eine Evaluation durch Schulfremde, d. h. über den Rahmen der Schulaufsicht hinaus, bedarf einer wohl durchdachten und widerspruchsfreien Regelung der *Einsichtsrechte* in *Lehrer-, Eltern- und Schülerdaten*. Ebenso dürfte eine Erweiterung der Eigenverantwortung dazu führen, dass die schulischen Gremien in verstärktem Umfang personenbezogene Daten zur Kenntnis nehmen müssen. Besonders bedenklich erscheint uns die Aufnahme schulfremder Personen in die *Schulkonferenz*. Im Weiteren teilten wir die in der öffentlichen Debatte vorgetragenen Bedenken bezüglich der *Eignungsprüfung der Schulleitung* und deren Bestellung. Der Entwurf sieht vor, dass einem großen Personenkreis ein Einsichtsrecht in die Bewerberdaten gegeben wird.

Endlich Normenklarheit bei der Sonderpädagogik

„Was lange währt, wird endlich gut“, gilt aus datenschutzrechtlicher Sicht für die kurz vor dem Erlass stehende *Verordnung über die Sonderpädagogische Förderung* (VO Sonderpädagogik). Seit langem mahnen wir eine derartige Regelung an[137]. Der derzeit vorliegende Zehnte Entwurf berücksichtigt unsere Empfehlungen. Die einzelnen Vorschriften legen normenklar fest, welche personenbezogenen Daten erhoben, verarbeitet und übermittelt werden dürfen. Um die datenschutzrechtlichen

[137] JB 1995, 5.9; JB 1996, 4.5.2; JB 1998, 4.5.2

Regelungen im Berliner Schulrecht jedoch nicht weiter in einzelnen Vorschriften zu separieren, sondern möglichst in der Schuldatenverordnung zu konzentrieren, regten wir an, diese zeitgleich mit dem Erlass der *Sonderpädagogikverordnung* zu ergänzen. Dabei geht es insbesondere um Befugnisse zur Führung und Aufbewahrung der sonderpädagogischen Bögen, die Verbindlichkeit einheitlicher Vordrucke[138], die Befugnisse zur Einsichtnahme in sonderpädagogische Förderbögen und den Umgang mit Unterlagen von Förderausschussverfahren, die nicht zu einer Förderung führten.

Schulen ans Netz

Die Ausstattung der Schulen mit Informationstechnik ist weltweit eines der großen Themen der Informationsgesellschaft. Allerdings hinkt hier Deutschland hinter anderen Ländern wie den USA hinterher: Während dort heute die Zielsetzung propagiert wird, jeden *Schülerarbeitsplatz* mit einem Rechner oder zumindest einem Rechneranschluss (bald werden sich die Schüler ihre Computer selbst mitbringen, wie sie es bereits von Taschenrechnern gewohnt sind) auszustatten, geht es in Berlin immer noch darum, die Schulen mit Rechnern auszustatten. Bei dem geplanten Neubau für eine Gesamtschule bedurfte es gleichwohl erheblicher Bemühungen der Schulleiterin zu erreichen, dass bei den Baumaßnahmen wenigstens Kabelkanäle in alle Unterrichtsräume gelegt werden (von den Kabeln selbst war noch gar nicht die Rede). Gleichwohl ist die Förderung des Computereinsatzes in der Schule Senatspolitik[139], das Projekt CidS ist Bestandteil des „Projekts Zukunft – Der Berliner Weg in die Informationsgesellschaft“[140]; „Mehr Mäuse an die Schule“ oder „Computer an @lle Schulen“ waren identische Forderungen der Koalitionsparteien im vergangenen Wahlkampf.

Einerseits ist der Computer künftig im *Unterricht* als Unterrichtsmittel nicht mehr wegzudenken. Andererseits werden Kenntnisse des Umgangs mit dem Computer, insbesondere aber auch der Anwendungsfelder, beginnend mit Rechen-, Datenverwaltungs- und Textverarbeitungsfunktionen bis hin zur Nutzung der vielfältigen Diensteangebote im Internet, unerlässliche Voraussetzungen für alle künftigen Berufe sein. Zu einem verantwortlichen Umgang mit dem Computer gehört es jedoch auch, die Anwendungsbedingungen und Folgen des Computereinsatzes zu kennen. Hierzu gehören die Rahmenbedingungen, die sich aus dem informationellen Selbstbestimmungsrecht, aber auch aus anderen Bereichen wie dem Urheberrecht oder dem Telekommunikations- und Teledienstерecht ergeben. Der Berliner Datenschutzbeauftragte hat schon seit vielen Jahren gefordert, den Datenschutz –

138 JB 1998, 4.5.2, S. 131
139 Abghs.-Drs. 13/3053
140 vgl. 2.2

nicht nur im Informatikunterricht, sondern auch in anderen Fächern – zum Unterrichtsgegenstand zu machen[141]. Abgesehen von individuellen Initiativen von Lehrern ist hierzu nichts geschehen. Dies muss sich vor dem Hintergrund der neuen Entwicklung ändern: Schulen ans Netz heißt auch, Schülerinnen und Schüler zu verantwortlichen Nutzern zu erziehen.

Auch beim derzeitigen Stand der Computernutzung an der Schule taucht eine Reihe datenschutzrechtlicher Fragen auf.

> *Während der Computereinsatz im Unterricht stark gefördert wird, werden für die Aufgaben der Schulverwaltung nur sehr zögerlich Geräte bereitgestellt. Dies weckt das Interesse aller, die Verwaltungsaufgaben in der Schule zu erledigen haben, die für den Unterricht beschafften Computer auch für Verwaltungsaufgaben zu nutzen.*

Derartige Wünsche, gleich ob Unterrichtscomputer selbst für Verwaltungszwecke genutzt oder Verwaltungs-PCs in das Schulnetz eingebunden werden, sind aus der Sicht des Datenschutzes nicht realisierbar. Selbst bei der Installation von Schutzvorkehrungen, die verhindern sollen, dass Schüler oder auch nicht befugte Lehrer Zugriff auf die Verwaltungsdaten nehmen, liegen darin erhebliche Risiken, die einen Verstoß gegen die Verpflichtung zur Einrichtung technisch-organisatorischer Maßnahmen begründen können (§§ 5, 11 Abs. 4 BlnDSG). Rechner, die für die Ausbildung vorgesehen sind, können nur schwer kontrolliert werden und genau dieses wird gerade von Schülern als Herausforderung gesehen, die Schutzmaßnahmen zu durchbrechen.

> *Nicht wenige Schulen verfügen über Internetzugänge und erlauben es ihren Schülern, persönliche E-Mail-Adressen zu nutzen. Darf ein Lehrer an Schüler gerichtete E-Mails lesen?*

Schulen mit einer derartigen technischen Ausstattung ist dringend zu empfehlen, durch eine *Benutzerordnung* Regeln für die Nutzung dieser Medien festzulegen. Wird beispielsweise vorgeschrieben, dass nur eine Kommunikation im Rahmen des Schulunterrichts zulässig ist, ohne dass private Nutzungsformen erlaubt werden, wird der Lehrer, schon um Anleitungen und Hinweise geben zu können sowie die Leistungen zu bewerten, die für den Unterricht gefertigte oder eingegangene „Post" einsehen müssen. Für die Schüler ist dann auch klar, dass es sich dabei nicht um ein Medium der Individualkommunikation handelt, sondern versandte Nachrichten ähnlich zu werten sind wie eine Wortmeldung während des konventionellen Unterrichts.

Wie verhält es sich jedoch, wenn die Schule den Schülern die Möglichkeit einer *privaten* Nutzung des Internet einräumt? Dabei fungiert die Schule als Anbieter von *Telediensten* im Sinne des Teledienstegesetzes. Damit ist die Verarbeitung von Verbindungs- und Nutzungsdaten

141 JB 1986, 4.4; 1994, 4.10

beschränkt (§ 6 TDDSG). Die Schule muss das Telekommunikations- bzw. Fernmeldegeheimnis für die von ihr bereitgehaltenen Nutzungsmöglichkeiten sichern. Der Lehrer hat nicht das Recht, bei einer privaten Nutzung ein- bzw. abgehende E-Mails der Schüler zu lesen. Daher sind die Schulen gut beraten, in einer Nutzerordnung anlassbezogene Kontrollverfahren festzuschreiben. Die Schüler und bei minderjährigen auch deren Eltern sind über dieses Verfahren zu informieren und ihre schriftliche Einwilligung in die Speicherung und Verwendung von Verbindungs- und Nutzungsdaten ist einzuholen. Eine Verweigerung der Einwilligung muss zu einer Sperrung der E-Mail-Adresse für private Kommunikationszwecke führen.

Einige Schulen haben ein eigenes Internet-Angebot. In einem dieser Angebote sollten in einer Liste die Namen der an der Erarbeitung dieses Angebots beteiligten Schüler veröffentlicht werden.

Das Internet-Angebot einer Schule stellt datenschutzrechtlich eine Veröffentlichung durch eine öffentliche Stelle des Landes Berlin dar. Internet-Veröffentlichungen sind nach dem Berliner Schulgesetz nur mit schriftlicher Einwilligung der Betroffenen, bei minderjährigen Schülern der Eltern, zulässig (§ 5 a). Das Problem liegt darin, dass der Verwendungszweck bei den potenziell weltweiten Nutzern dieses Angebots nicht bestimmt werden kann. Die Einwilligungserklärung muss also diese Risiken deutlich benennen und über sie aufklären. Erst dann ist mit Wissen und Wollen der Schüler und ihrer Eltern ein solcher Eintrag auch in das Impressum zulässig.

4.5.3 Statistik

Während wir im Jahresbericht 1998 noch davon ausgingen, dass sich Deutschland am europäischen *Zensus* im Jahr 2001 beteiligen wird[142], ist seit März 1999 klar, dass zwar auf Grundlage von Fortschreibungsdaten versucht wird, den Anforderungen der EU zu genügen, eine *Volkszählung* jedoch noch nicht stattfinden wird. Die Bundesregierung hat sich entschlossen, den angestrebten Methodenwechsel von der direkten Befragung der gesamten Bevölkerung zu einer registergestützten Zensuserhebung mit punktueller Befragung gründlicher vorzubereiten. Zu diesem Zweck hat eine Arbeitsgruppe der Statistischen Ämter von Bund und Ländern für die amtliche Statistik im Jahr 1999 Vorschläge für ein Testgesetz erarbeitet. Mittels einer hinreichend großen Stichprobe sollen zunächst neue Verfahren der Registerauswertung und Zusammenfügung erprobt werden. Dabei sollen die unterschiedlichen Vorschläge des früheren Bundes- wie Ländermodells berücksichtigt werden[143].

142 JB 1998, 4.5.3
143 JB 1997, 4.5.3

Ziel ist es, die Test- und Qualitätsuntersuchungen noch in der laufenden Legislaturperiode des Bundestages durchzuführen und auszuwerten. Die datenschutzrechtlichen Probleme einer *Registerzusammenführung* bedürfen dabei noch einer vertieften Diskussion. Wenn sowohl die rechtlichen als auch die methodischen Probleme lösbar sind, könnte in der nächsten Legislaturperiode ein Volkszählungsgesetz erlassen und ein Zensus durchgeführt werden.

4.6 Wirtschaft

4.6.1 Banken und Versicherungen

Der gläserne Aktionär

Deutsche Aktiengesellschaften tendieren verstärkt dazu, anonyme Inhaberaktien auf die im internationalen Wertpapierhandel dominierende „Namensaktie" umzustellen. Die Vorschriften des Aktiengesetzes können jedoch bei der Einführung von Namensaktien zu problematischen datenschutzrechtlichen Konsequenzen führen. Einer Petentin, die nicht mit ihrem Namen, Wohnort und Beruf im Aktienbuch verzeichnet sein wollte und stattdessen ihr Kreditinstitut als Depotbank dort eintragen lassen wollte, wurde dies durch ihre Bank verweigert.

Bei den bislang in Deutschland gebräuchlichen Inhaberaktien ist den *Aktiengesellschaften* die Identität ihrer Aktionäre regelmäßig nicht bekannt, wohingegen *Namensaktien* nach den Bestimmungen des Aktiengesetzes unter Bezeichnung des Inhabers nach Namen, Wohnort und Beruf in das *Aktienbuch* der Gesellschaft einzutragen sind (§ 67 Abs. 1 Aktiengesetz (AktG)). Problematisch ist dies aus datenschutzrechtlicher Sicht aus zwei Gründen: Zum einen kann nach § 67 Abs. 5 AktG jeder Anteilseigner Einsicht in das Aktienbuch nehmen. Hierfür reicht der Erwerb nur einer Aktie aus. Zum anderen finden sich im Aktiengesetz keine datenschutzrechtlichen Bestimmungen zum Umgang mit den im Aktienbuch aufgeführten personenbezogenen Daten der Aktionäre durch die Gesellschaft, so dass auf die allgemeinen Regelungen des BDSG zurückgegriffen werden muss.

Die Einsichtnahme in das Aktienbuch ist jedem Aktionär ohne Nachweis eines besonderen Interesses zu gewähren (§ 67 Abs. 5 AktG). Das Gesetz schränkt somit die Möglichkeit, sich Kenntnis über seine Mitaktionäre zu verschaffen, nicht ein. Die Aktiengesellschaften können allerdings sowohl in inhaltlicher als auch in organisatorischer Hinsicht die Möglichkeiten zur Einsichtnahme begrenzen. Die Daten der Aktionäre werden bei den verschiedenen Gesellschaften, die im Laufe dieses Jahres ihren Bestand auf Namensaktien umgestellt haben, ganz unterschiedlich aufgeführt. So wird unter dem Merkmal „Wohnort" nicht bei allen Gesellschaften die komplette Adresse, sondern nur die Stadt angegeben. Hinsichtlich der beruflichen Tätigkeit wird meist eine Eintragung nach Kategorien wie „Angestellter", „Selbständig", „Beamter"

oder „Hausfrau“ vorgenommen. Zwar führen fast alle Unternehmen im Aktienbuch noch weitere als die in § 67 Abs. 1 AktG genannten Daten, wie z. B. die Gesamtstückzahl, Fremd- oder Eigenbesitz, Datum des An- bzw. Verkaufs, letztes Bewegungsdatum oder Nationalität des Aktionärs, auf, jedoch werden Daten wie Beruf und Nationalität dabei teilweise verschlüsselt angegeben und sind für den Einsicht nehmenden Aktionär nicht identifizierbar. In einem Referentenentwurf des Bundesministeriums für Justiz zum Namensaktiengesetz (NAstraG) soll auf die Berufsangabe verzichtet werden. Dies ist schon deshalb sinnvoll, da sie gerade – wenn nur eine sehr grobe Einteilung vorgenommen wird – wenig aussagekräftig ist. Das nach dem Aktiengesetz nicht vorgesehene Merkmal „Nationalität“ ist hingegen erforderlich, wenn die Gesellschaft, um als nationale Gesellschaft anerkannt zu werden, mindestens zur Hälfte deutsche Anteilseigner aufweisen muss.

Auch die von den Aktiengesellschaften angebotenen Modalitäten der Einsichtnahme begrenzen die Möglichkeit des „Ausspionierens“ von Mitaktionären. Einsicht in das Aktienbuch wird nur in den Geschäftsräumen des Unternehmens unter Aufsicht von Mitarbeitern gewährt. Verlangt werden kann nur ein Ausdruck der eigenen Daten, nicht aber eine Kopie des gesamten Aktienbuchs. Zwar ist jedem Aktionär Einsicht in das gesamte Aktienbuch zu gewähren (§ 67 Abs. 5 AktG), in der uns bisher bekannten Praxis der Gesellschaften war es aber nicht möglich, das Aktienbuch nach einer bestimmten Person zu durchsuchen. Teilweise werden per Zufallsgenerator die Daten eines beliebigen Aktionärs eingespielt, bei der Sortierung nach Aktien oder Aktionärsnummern erscheinen die Namen in beliebiger Reihenfolge. Eine Invertsuche nach Namen ist nicht möglich. Bei keiner der von uns befragten Gesellschaften wird dem Aktionär im Rahmen einer Einsichtnahme die Möglichkeit der Auswertung nach bestimmten Suchfunktionen gewährt. Ihm wird lediglich das Recht eingeräumt, das Aktienbuch „durchzublättern“, d. h. sich nacheinander Seite für Seite anzuschauen. Dies entspricht auch dem Sinn und Zweck der Regelung des § 67 Abs. 1 AktG, die es dem Aktionär einerseits zwar ermöglichen soll, sich über seine Mitaktionäre zu informieren, andererseits stellt das Aktienbuch aber ein internes Dokument der Gesellschaft dar, dessen Einsichtsrecht gerade nicht mit dem eines öffentlich zugänglichen Registers vergleichbar ist.

Grundsätzlich können alle Aktionäre, die anonym bleiben wollen, ihre Depotbank oder einen anderen Treuhänder benennen, der statt ihrer als Fremdbesitzer im Aktienbuch verzeichnet wird. In unserem Fall stellte sich heraus, dass die Weigerung der Bank, sich als Treuhänder in das Aktienbuch eintragen zu lassen, nur auf Unkenntnis des betreffenden Mitarbeiters beruhte.

Ziel kann es jedoch nicht sein, sämtlichen Aktionären, die ihre persönlichen Daten der Gesellschaft und/oder den Mitaktionären nicht

offenbaren wollen, lediglich die Möglichkeit einzuräumen, ihre Depotbank als Anteilseigner eintragen zu lassen, zumal ein solcher Eintrag nicht nur mit finanziellen Nachteilen verbunden ist. Gegenüber der Gesellschaft gilt nur derjenige als Aktionär, der auch im Aktienbuch eingetragen ist (§ 67 Abs. 2 AktG). Eine Teilnahme an der Hauptversammlung bzw. eine Ausübung des Stimmrechts setzt eine entsprechende Bevollmächtigung durch die depotführende Bank voraus. Die bisher zufrieden stellende Praxis der Aktiengesellschaften ändert nichts daran, dass es aus datenschutzrechtlicher Sicht zu begrüßen wäre, wenn die Einsichtsmöglichkeiten der Aktionäre insgesamt eingeschränkt werden und der Aktionär zukünftig nur noch in die ihn betreffenden Eintragungen Einsicht verlangen kann. Der Referentenentwurf sieht eine entsprechende Einschränkung vor.

Eine Beschränkung des Einsichtsrechts der Aktionäre schützt diese jedoch nicht vor *Nutzung* ihrer personenbezogenen Daten durch das Unternehmen. Sämtliche Aktienbücher der großen Gesellschaften werden elektronisch geführt. Zwar sind die Aktienbücher unterschiedlich aufgebaut, d. h. größtenteils nach Aktionärsnummern, teilweise auch nach Aktiennummern sortiert. Jedes dieser elektronisch geführten Aktienbücher bietet der Gesellschaft jedoch die Möglichkeit, die Daten ihrer Aktionäre gezielt auszuwerten und so Erkenntnisse über die Aktionärsstruktur zu erhalten. Wie ist die soziale Schichtung? Wie hoch ist die Anzahl der ausländischen Aktionäre? Wann kauft ein Aktionär Aktien? Zu welchem Zeitpunkt verkauft er wieder? Welche Besitzintervalle liegen vor? Die elektronische Auswertung ermöglicht die Erstellung von Bewegungslisten zu einzelnen Aktionären.

Im Aktiengesetz findet sich bisher keine Datenschutzbestimmung, die die Nutzung der im Aktienbuch enthaltenen personenbezogenen Daten durch die Gesellschaft – z. B. zu Werbezwecken oder zur Erstellung einer Aktionärsdemographie – regelt. Nach dem Bundesdatenschutzgesetz darf eine Aktiengesellschaft die Daten aus dem Aktienbuch nur im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit ihren Aktionären nutzen (§ 28 Abs. 1 Satz 1 Nr. 1). Die elektronischen Auswertungsmöglichkeiten dürfen also nur insoweit genutzt werden, wie es dem Zweck des Aktienbuchs entspricht. Das Aktienbuch dient u. a. dazu, die Gesellschaft über ihre Aktionäre zu informieren. Eine Nutzung der Aktionärsdaten im Rahmen der Investor-Relations-Tätigkeit der Gesellschaft ist daher grundsätzlich zulässig. Wir würden es begrüßen, wenn der Gesetzgeber in dem Namensaktiengesetz eine abschließende (bereichsspezifische) Regelung zur Nutzung und Verarbeitung der Aktionärsdaten treffen würde. Hierbei sollte insbesondere auch geregelt werden, dass die Gesellschaft die personenbezogenen Daten des Aktionärs nicht an Dritte für Zwecke der Werbung übermitteln darf.

4.6.1

Die umfangreiche Selbstauskunft

Ein Petent beschwerte sich, dass er bei seinem Antrag auf Eröffnung eines Girokontos einen umfangreichen Selbstauskunftsbogen ausfüllen sollte, der von dem Kreditinstitut gleichzeitig zur Bonitätsprüfung bei Kredit- oder Leasingverträgen verwendet wird. Mittels dieses Selbstauskunftsbogens werden Daten zu Nationalität, Wehrdienst, Familienstand, Namen des Ehegatten sowie detaillierte Angaben zum monatlich verfügbaren Einkommen, Guthaben/Wertpapierdepots, Lebensversicherungen, Bausparverträgen, Grundbesitz und sonstigen Vermögenswerten erhoben. Der Selbstauskunftsbogen enthält ferner eine Einwilligungserklärung, die das Kreditinstitut berechtigt, „jederzeit die öffentlichen Register sowie das Grundbuch und die Grundakten einzusehen und einfache oder beglaubigte Abschriften und Auszüge zu beantragen, ebenso Auskünfte bei Versicherungen, Behörden und sonstigen Stellen, insbesondere Kreditinstituten einzuholen, die es zur Beurteilung des entsprechenden Antrags für erforderlich halten darf".

Bei einem Antrag auf Eröffnung eines *Girokontos* kommt nur ein Speichern von Daten in Frage, die für einen späteren Vertragsschluss erforderlich sind (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Die speichernde Stelle muss sich dabei auf die Verwendung der für den konkreten Vertragszweck erforderlichen Daten beschränken. Die Vertragszwecke von Giro- und Kreditverträgen unterscheiden sich erheblich voneinander, so dass eine Bank bei einem *Kreditvertrag* umfangreichere Daten zu den Vermögensverhältnissen des Kunden speichern darf.

Das Kreditinstitut verwendet das Formular sowohl für Giro- als auch für Kreditverträge. Es hat zwar darauf hingewiesen, dass es von Kunden, die nur ein Girokonto eröffnen möchten, nicht die gesamten im Formular vorgesehenen Angaben benötigt. Dies ist dem Formular selbst jedoch nicht zu entnehmen. Das äußere Erscheinungsbild des Formulars lässt eher vermuten, dass es im Ermessen des einzelnen Bankmitarbeiters liegt, welche konkreten Daten er von dem Kunden erhebt. Künftig sollten zwei getrennte Selbstauskunftsbögen für Girokontoeröffnungen und Kreditverträge verwendet werden.

Angaben zum Beruf, zur Nationalität, zum Familien- bzw. Güterstand sowie zum *Wehrdienst* sind für die Ausführung eines Girovertrages für das Kreditinstitut nicht relevant. Die Speicherung dieser Daten ist daher unzulässig. Dies gilt für das Datum „Wehrdienst" auch im Falle eines Kreditvertrages, da es zur Prüfung der Bonität für das Kreditinstitut irrelevant ist, ob der zukünftige Vertragspartner seinen Wehrdienst abgeleistet hat oder nicht.

Detaillierte Angaben zum monatlichen Einkommen sowie zu den Vermögenswerten sind bei Eröffnung eines Girokontos auch im Falle der Einräumung eines Dispositionskredites nicht erforderlich. Es ist üblich, dass dem Neukunden zunächst eine geringe Kreditlinie einge-

räumt wird, die später entsprechend der Höhe der monatlichen Eingänge erhöht wird. Zur Sicherheit des zunächst eingeräumten niedrigen Dispositionskredites genügt die Angabe, ob der Antragsteller regelmäßige monatliche Einkünfte hat. Die Art der Einkünfte ist dabei irrelevant. Anders stellt sich die Situation im Fall eines Kredit-/Leasingvertrages dar, da hier die Bank eine Leistung erbringt, für die entsprechende Sicherheiten durch den Antragsteller zur Verfügung gestellt werden müssen.

Die Einwilligungserklärung, welche das Kreditinstitut berechtigt, jederzeit das *Grundbuch* und die Grundakten einzusehen und einfache oder beglaubigte Abschriften und Auszüge zu beantragen, ist bei Eröffnung eines Girokontos gleichfalls unzulässig. Nach § 12 Grundbuchordnung ist die Einsicht in das Grundbuch nur bei Darlegung eines berechtigten Interesses gestattet. Ein berechtigtes wirtschaftliches Interesse des Kreditinstitutes ist abzulehnen, da eine Kreditgewährung nicht in Aussicht steht und somit auch keine entsprechenden Sicherheiten durch den Antragsteller angeboten werden müssen. Erst recht unzulässig ist daher das Beantragen von einfachen oder beglaubigten Abschriften und Auszügen aus dem Grundbuch und den Grundakten. Die Einwilligungserklärung in die Einsichtnahme in das Grundbuch durch die Bank stellt eine unzulässige Datenerhebung dar, da Daten, die der Bank gerade nicht zugänglich sind, ihr mit Hilfe einer Selbstauskunftserklärung des Antragstellers zugänglich gemacht werden sollen.

Der weitere Teil der *Einwilligungserklärung,* durch welchen das Kreditinstitut ermächtigt wird, Auskünfte bei Versicherungen, Behörden und sonstigen Stellen einzuholen, die zur Beurteilung des Kredit-/Leasingantrages für erforderlich gehalten werden, ist in dieser allgemeinen Formulierung unzulässig. Hier ist den Betroffenen nicht klar, in welche öffentlichen Register Einsicht genommen und bei welchen Versicherungen, Kreditinstituten und Behörden angefragt werden soll. Vor der Entscheidung über einen Kreditantrag kann es im Einzelfall zwar erforderlich sein, weitere Informationen von anderen Stellen einzuholen, dennoch muss dem Betroffenen bei Abgabe seiner Einverständniserklärung auch immer die Tragweite seiner Einwilligung bewusst sein (§ 4 Abs. 1 BDSG), d. h. ihm müssen die Stellen, von denen weitere Daten abgefragt werden sollen, genau benannt werden. Die pauschal gehaltene Einwilligungserklärung des Selbstauskunftsbogens nimmt dem Betroffenen die Möglichkeit, das Ausmaß seiner Einwilligung zu überblicken, und ist daher mit § 4 Abs. 1 BDSG nicht vereinbar.

Das Kreditinstitut ist unseren Hinweisen bisher nicht gefolgt.

Eine Kontonummer zu viel

Wir wurden darauf aufmerksam gemacht, dass zwei Kreditinstitute ihren Kunden auf allen Kontoauszügen als Empfänger einer Gutschrift neben dem Namen des Einzahlers auch dessen Kontonummer mitteilen.

Aus der Kontonummer können Rückschlüsse darüber gezogen werden, ob es sich um ein laufendes Konto, ein Girokonto, ein Unterkonto, ein Kreditkonto oder ein Sparkonto handelt.

Bei der Mitteilung von Namen und *Kontonummer* des Einzahlers auf den *Kontoauszügen* des Empfängers handelt es sich um eine Datenübermittlung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Die vertragliche Zweckbestimmung gibt vor, welche Daten übermittelt werden dürfen. Eine Datenübermittlung, die zur Verwirklichung des Vertragszwecks nicht erforderlich ist, ist somit unzulässig.

Zur Ausführung des *Überweisungsauftrags* ist es nicht erforderlich, dem Überweisungsempfänger die Kontonummer des Einzahlers zur Kenntnis zu bringen. Zur Identifizierung eines Überweisungsauftrages ist es ausreichend, dass der Name des Einzahlers, der von ihm angegebene Verwendungszweck – so wie er auf dem dafür vorgesehenen Feld des Überweisungsträgers angegeben ist – sowie die Höhe des zu überweisenden Betrages auf dem Kontoauszug des Empfängers erscheinen. Für den Empfänger der Zahlung sind diese Daten ausreichend, um den Zahlungsbetrag auf seinem Konto einer bestimmten Person zuordnen zu können.

Wir haben beide Kreditinstitute auf die Unzulässigkeit der Übermittlung der Kontonummer des Einzahlers an den Geldempfänger hingewiesen, woraufhin eines der Kreditinstitute sich sofort an den zuständigen Bundesverband wandte. Der Bundesverband Öffentlicher Banken Deutschlands hat sich daraufhin bereit erklärt, die ihm angeschlossenen Kreditinstitute zu bitten, künftig bei den papiergebundenen Kontoauszügen im Datenträgeraustausch die Angabe der Kontonummer des Auftraggebers zu unterdrücken. Auf den Kontoauszügen dieses Kreditinstituts erscheint die Kontonummer des Einzahlenden nicht mehr. Das andere Kreditinstitut hat unseren Hinweis bisher leider nicht umgesetzt.

Patientennamen im Zahlungsverkehr

Ein Arzt machte darauf aufmerksam, dass im Zahlungsverkehr mit Versicherungen Patientendaten offenbart werden. Denn auf dem Überweisungsträger der Versicherung, den der Arzt durch sein Kreditinstitut erhält, sei der Name des Patienten und der Grund für die ärztliche Untersuchung vermerkt.

Es handelte sich dabei um die Abrechnungsvorgänge im Rahmen einer ärztlichen Begutachtung, also das *Arzthonorar* für den externen ärztlichen Gutachter, der für eine private Versicherung tätig geworden ist.

Wenn ein Arzt für die Begleichung seiner Kosten eine Rechnungsnummer und/oder ein Buchungskennzeichen angab, hat die Versiche-

rung seine Gebühren nur unter Angabe dieser *„Buchungszeichen"* überwiesen. Die Versicherung räumte allerdings ein, dass dies die Ausnahme sei, weil die Ärzte auf ihren Kostenabrechnungen nur selten solche Buchungsdaten angäben. Die Ärzte erwarten jedoch auf der Überweisung einen Verwendungszweck, der ihnen eine Zuordnung der überwiesenen Geldbeträge in der eigenen Buchhaltung ermöglicht. Im Regelfall wird dann, wenn keine anonymen Buchungszeichen angegeben werden, der Name des Kunden (Patienten) sowie eine sehr allgemein formulierte Angabe (z. B. „Untersuchung vom . . ." oder „Gutachten vom . . .") verwendet. Ein konkreter Untersuchungsgrund oder Anlass sollte nicht genannt werden. Auf unsere Anregung hat das betroffene Versicherungsunternehmen veranlasst, dass die Fragebögen und seitens der Versicherung vorbereitete Druckstücke in der Form ergänzt werden, dass die Versicherung ausdrücklich darum bittet, ihr die für die Begleichung der Rechnung erforderlichen Buchungszeichen zu benennen, damit diese auf der Überweisung als Verwendungszweck angegeben und auf den Namen des Patienten verzichtet werden könne. Allerdings bleibt für den Fall, dass ein Arzt insoweit nicht mitwirkt, der Versicherung nichts anderes übrig, als unter dem Kundennamen des Patienten die Arztrechnung zu begleichen. Dann liegt das Verschulden jedoch nicht bei der Versicherung, sondern in der nachlässigen Handhabung des Arztes selbst.

Die PIN-Eingabe erst ganz zum Schluss

Bei den Selbstbedienungsterminals der Landesbank Berlin erfolgt die Aufforderung zur Eingabe der Persönlichen Identifikationsnummer (PIN) erst dann, wenn konkrete Verfügungen an einem Konto bestätigt werden sollen. Die Abfrage von Informationen zum Konto wie Kontostand, bestehende Daueraufträge und spezielle regelmäßige Überweisungen ist nach Einstecken der ec- oder S-Karte ohne weitere Authentifizierung möglich. Die Bürger befürchten, dass nach Diebstahl oder Verlust der Karte Dritten Informationen über ihre finanziellen Verhältnisse, ihr Finanzgebaren und persönliche Gewohnheiten offenbart werden könnten.

Die Befürchtungen sind nicht von der Hand zu weisen. Daueraufträge geben zum Beispiel Informationen über sachliche Verhältnisse, die zur regelmäßigen Zahlung führen wie Mieten, Wohngelder, Mitgliedsbeiträge in Vereinen jeglicher Art, regelmäßige Unterstützungen, Unterhaltszahlung und manches mehr. Aus den Angaben, die unter Verwendung einer gestohlenen Karte abgefragt werden können, könnten Rückschlüsse gezogen werden, die zur Beurteilung von Ertrag und Risiken von Straftaten (Einbruch, Entführung etc.) geeignet sein könnten.

Zwar ermöglichen es alle Kreditinstitute, an *Kontoauszugsdruckern* ohne Eingabe einer Geheimzahl Kontoauszüge abzurufen, was einer

angeblich der Kundenfreundlichkeit dienenden bundesweiten Vorgabe des Zentralen Kreditausschusses (ZKA) entspricht. Die Praxis an den *Selbstbedienungsterminals* der Landesbank Berlin geht aber weit darüber hinaus und wird bei den von uns geprüften anderen Kreditinstituten in Berlin anders gehandhabt. Dort wird die PIN nach dem Einschieben der Karte verlangt. Auch die Preisgabe der weiteren Informationen zum Konto ist somit erst nach dieser weiteren Authentifizierung möglich.

Die Landesbank Berlin war der Auffassung, dass sie gegen keine datenschutzrechtlichen Bestimmungen verstößt. Nachdem wir darauf hingewiesen hatten, dass die festgestellte Praxis ein nicht unerheblicher Mangel der Speicherkontrolle nach § 5 Abs. 3 Nr. 3 BlnDSG ist und somit sehr wohl im Widerspruch zu datenschutzrechtlichen Bestimmungen steht, stufte die Bank im August 1998 die mit der späten PIN-Eingabe verbundenen Risiken als „sehr klein" ein, bekundete aber ihr starkes Eigeninteresse an einem hohen Datenschutzstandard. Mit der Erweiterung der Datenbereitstellungen an den Terminals sei die Vorverlagerung der *PIN-Prüfung* vorgesehen. Wegen der vorrangigen Arbeiten zur Umstellung auf den EURO und der Maßnahmen gegen das Jahr-2000-Problem sei die Programmierung jedoch auf Frühjahr 1999 verschoben worden.

Dabei hatte die Landesbank jedoch die Rechnung ohne die Datenverarbeitungsgesellschaft (dvg) Hannover gemacht, ein Unternehmen, welches für die norddeutschen Sparkassen die Entwicklung und Betreuung der IT-Verfahren durchführt. Noch im März 1999 waren die Kapazitäten der dvg Hannover mit dem EURO und dem Y2K-Problem dermaßen belastet, dass eine Lösung des Problems erst im Herbst zu erwarten war. Wir haben daraufhin unsere Missbilligung zum Ausdruck gebracht, dass die dvg dem Datenschutz und der informationstechnischen Sicherheit zugunsten der Kunden nicht die gesetzlich gebotene Priorität einräumt. Nachdem die Realisierung im Herbst noch einmal bekräftigt, dann auf Ende November verschoben worden war, ergab eine Kontrolle im Dezember keine Veränderungen. Allerdings war die Landesbank mit Kräften bemüht, ihren Programmier-Auftragnehmer dvg von der Dringlichkeit der Änderung zu überzeugen, zumal das erweiterte Informationsangebot mit der Jahr-2000-Umstellung verfügbar sein sollte. Inzwischen liegt uns die Mitteilung vor, dass Mitte Januar 2000 die Vorverlagerung der PIN-Eingabe in einigen Filialen im Pilotversuch erprobt und nach erfolgreichem Abschluss eingeführt werden soll.

4.6.2 Auskunfteien

Teure Selbstauskünfte

Mehrere Bürger haben angefragt, ob es zulässig ist, dass die Schutzgemeinschaft für allgemeine Kreditauskünfte (SCHUFA) für schriftlich

erteilte Selbstauskünfte, die der Betroffene lediglich zur Überprüfung der Richtigkeit der bei der SCHUFA über ihn gespeicherten Daten einholt, eine Gebühr erhebt. Ein Bürger hat angezweifelt, ob die Höhe des Entgelts von 15,00 DM den tatsächlichen Kosten einer solchen Auskunft entspricht, und hat vor dem Landgericht Berlin auf Rückzahlung von 12,00 DM pro bezahlte Selbstauskunft gegen die SCHUFA geklagt.

Die speichernde Stelle hat eine *Auskunft* zu den gespeicherten Daten grundsätzlich kostenlos zu erteilen (§ 34 Abs. 5 Satz 1 BDSG). Die gebührenpflichtige Auskunft stellt schon nach dem Gesetzeswortlaut eine Ausnahme dar (§ 34 Abs. 5 Satz 2 BDSG). Von § 34 Abs. 5 Satz 2 BDSG sollte die speichernde Stelle daher nur sehr eingeschränkt Gebrauch machen, zumal eine Entgeltlichkeit der Auskunft den Betroffenen in der Wahrnehmung seiner Rechte behindert. Was die *SCHUFA* betrifft, so soll durch diese Entgeltregelung vor allem verhindert werden, dass z. B. eine Bank auf die für sie mit Kosten verbundene Abfrage bei der SCHUFA verzichtet und stattdessen die Kundin bzw. den Kunden veranlasst, die kostenlose Selbstauskunft einzuholen.

Gegen eine grundsätzliche Entgeltverpflichtung bei der Einholung einer schriftlichen SCHUFA-Selbstauskunft bestehen Bedenken. Nach § 34 Abs. 5 Satz 2 BDSG darf ein Entgelt für eine Auskunft von Auskunfteien nur erhoben werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Auskunfteien und Kreditinformationseinrichtungen sind also nicht befugt, generell darauf zu verweisen, dass die Daten auch als „Selbstauskunft" zu kommerziellen Zwecken verwendet werden könnten. Vielmehr muss für die Auskunftei erkennbar sein, dass der Betroffene unmittelbar und in einem konkreten Fall die Auskunft zu wirtschaftlichen Zwecken beantragt. Fordert ein Bürger eine Selbstauskunft zur Überprüfung der Richtigkeit des Datensatzes an, so geschieht dies ausschließlich zu persönlichen Zwecken ohne kommerzielle Verwendungsabsicht. In diesem Fall ist die Erhebung einer Gebühr unzulässig.

Aber auch bei einer *Selbstauskunft,* die der Betroffene zu wirtschaftlichen Zwecken einholt, dürfen bei der Festlegung der Höhe des Entgelts nur die direkt zurechenbaren Kosten berücksichtigt werden (§ 34 Abs. 5 Satz 3 BDSG). Hierzu zählen z. B. die Selbstkosten für Material und Porto sowie anteilige Maschinen- und Personalkosten für die Zeit, welche durch die Auskunftserteilung aufgewendet wird. Die speichernde Stelle muss in jedem Fall in der Lage sein, die Zusammensetzung des Entgelts der Aufsichtsbehörde im Einzelnen nachzuweisen.

Das Landgericht Berlin hat die Höhe von 15,00 DM pro SCHUFA-Selbstauskunft für unzulässig erklärt, da allgemeine Verwaltungs- und Betriebskosten in die Höhe des Entgelts nicht mit einzubeziehen sind und ein Gewinn mit der Auskunft nicht erzielt werden darf[144]. Der

144 Urteil v. 14. 1. 1999, Az.: 14 O 417/97

Petent hatte unter Vorlage eines Jahresberichts der SCHUFA aus dem Jahre 1996 nachgewiesen, dass die tatsächlichen Kosten pro Auskunft deutlich unter 1,00 DM lagen, und die allgemeine Kostensteigerung mit 2,00 DM berücksichtigt. Dieses Urteil gilt nur zwischen den Parteien, d. h., andere Gerichte sind an dieses Urteil nicht gebunden. Die Bundes-SCHUFA hat uns mitgeteilt, dass sie in jedem nachfolgenden Gerichtsverfahren ein Gutachten vorlegen werde, nach dem die tatsächlich anfallenden Kosten pro Selbstauskunft deutlich über 15,00 DM liegen. Das Einbringen des Gutachtens in den Prozess wurde von den Anwälten der SCHUFA versäumt. Die Bundes-SCHUFA ist daher auch nach dem Urteil nicht bereit, das Entgelt pro Selbstauskunft zu reduzieren.

Nachbarschaftsbefragungen

Sofern ein Unternehmen bei einer Auskunftei eine Bonitätsauskunft zu einem Vertragspartner einholen möchte und bei der Auskunftei noch kein Datensatz zu dieser Person existiert, entsendet die Auskunftei Außendienstmitarbeiter, die Informationen über die Kreditwürdigkeit des Betroffenen einholen sollen. Zahlreiche Bürger haben sich darüber empört, dass diese Außendienstmitarbeiter Nachbarn, Hausmeister oder Postboten zu ihren finanziellen Verhältnissen und Einkünften befragen, ohne dass sie als Betroffene selbst davon Kenntnis erhalten. In einem Fall hatte ein Nachbar angegeben, der Betroffene sei arbeitslos, da er tagsüber immer in der Wohnung anzutreffen ist. Tatsächlich ist der Petent freiberuflich tätig.

Wir halten eine solche Recherche im persönlichen Umfeld des Betroffenen ohne seine Mitwirkung für unzulässig. Diese Datenerhebung hat nach *Treu und Glauben* und auf rechtmäßige Weise zu erfolgen (§ 29 Abs. 1 Satz 2 i. V. m. § 28 Abs. 1 Satz 2 BDSG). Auch im nichtöffentlichen Bereich ist vom Vorrang der Direkterhebung beim Betroffenen auszugehen. Nur in Ausnahmefällen kann eine Datenerhebung beim Betroffenen unterbleiben, etwa wenn eine solche mit unverhältnismäßigem Aufwand verknüpft sein sollte und keine Anhaltspunkte für eine Beeinträchtigung schutzwürdiger Interessen des Betroffenen vorliegen (vgl. § 13 Abs. 2 Satz 2 Nr. 2 b BDSG).

Bei dieser Recherchemethode werden schutzwürdige Belange des Betroffenen beeinträchtigt, da Dritte über die Bonitätsprüfung informiert werden und zudem regelmäßig die Gefahr besteht, dass *Nachbarn* zu Spekulationen veranlasst werden, die sich nachteilig auf den Betroffenen auswirken. Insbesondere bei Bagatellfällen, d. h. bei Konsumentenkrediten mit geringem Kreditvolumen, steht diese Beeinträchtigung in keinem angemessenen Verhältnis zum berechtigten Interesse des Auskunfteikunden. Derartige Recherchen im persönlichen Umfeld des Betroffenen zum Zwecke der Erteilung von Kreditauskünften im Rahmen des Konsumentenkredits sind unverhältnismäßig und damit unzulässig.

Wo kommen all die Daten her?

Ein Polizeimitarbeiter hat unbefugt Daten aus dem Informationssystem Verbrechensbekämpfung (ISVB) abgefragt und Daten über Ermittlungsverfahren von Betroffenen einer Detektei/Auskunftei zur Verfügung gestellt, die die Daten wiederum an einen Auftraggeber weitergegeben hat. In den Akten der Detektei sind keine Hinweise auf die Herkunft der Daten enthalten. Die unbefugte Datenweitergabe durch einen Mitarbeiter der Polizei kam nur durch eine Recherche bei den Protokollen zu ISVB-Abfragen ans Licht.

Dieser Fall zeigt deutlich, wie notwendig es ist, dass für Auskunfteien und Detekteien eine gesetzliche *Aufzeichnungspflicht für Datenquellen* geschaffen wird. Das BDSG enthält bisher keine explizite Regelung bezüglich einer solchen Dokumentationspflicht. Dies hat zur Folge, dass ein nach § 34 Abs. 1 BDSG bestehender Auskunftsanspruch des Betroffenen hinsichtlich der Herkunft der zu seiner Person gespeicherten Daten ins Leere läuft, wenn die speichernde Stelle die Datenquelle nicht dokumentiert hat.

Nach der aufgehobenen Auskunftei- und Detekteiverordnung bestanden weit reichende Aufzeichnungspflichten, insbesondere zur Person des Auftraggebers, zum Umfang des erteilten Auftrags, zu den Ergebnissen der Einzelermittlung, nicht jedoch zur Herkunft der ermittelten Daten. Der Gesetzgeber hat jedoch stattdessen eine Ermächtigung für die Länder vorgesehen, entsprechende Verordnungen zu erlassen (§ 38 Abs. 3 Gewerbeordnung). Die Senatsverwaltung für Wirtschaft und Betriebe hat Bereitschaft zum Erlass einer solchen Verordnung signalisiert. Mit einer neu geschaffenen Verordnung wären Auskunftsansprüche der Betroffenen gegenüber Auskunfteien und Detekteien deutlich besser realisierbar.

4.6.3 Verkehrsunternehmen

Deutsche Bahn AG

Die *Deutsche Bahn AG* (DB), die ihren Unternehmenssitz in Berlin hat, ist das größte Unternehmen in unserem Zuständigkeitsbereich. Ihr gilt daher unsere besondere Aufmerksamkeit, seit wir die Aufgaben der Aufsichtsbehörde übernommen haben.

BahnCard goes home

Das Projekt der DB, die bereits seit Jahren eingeführte *BahnCard* ab Mitte 1995 gemeinsam mit der *Citibank* zu produzieren und mit einer Kredikartenfunktion zu verbinden, hatte zu einer erregten öffentlichen Diskussion über den hinreichenden Schutz der Daten bei der Verarbeitung in den *USA* geführt. Bei der Übernahme der Aufgabe der Auf-

sichtsbehörde fanden wir dieses Problem vor. Der DB und der Citibank war daran gelegen, durch geeignete juristische und technische Maßnahmen ein Höchstmaß an Datenschutzvorkehrungen für die Kunden zu gewährleisten. Im Ergebnis wurde mit einer Vereinbarung zwischen DB und den deutschen und amerikanischen Citibank-Organisationen ein Weg gefunden, der noch heute in der internationalen Datenschutzgemeinde für vorbildlich bei derartigen Vereinbarungen gehalten wird[145].

Gegenstand der Vereinbarung war die Verarbeitung personenbezogener Daten der BahnCard- sowie der entsprechenden Kreditkartenkunden, die in den Rechenzentren der Citibank in Sioux Falls, South Dakota, und Las Vegas, Nevada, stattfinden sollte. Insbesondere handelte es sich um die technische Herstellung der BahnCard (Las Vegas) sowie die Entscheidung über die Zulassung der Kreditkartenfunktion (Sioux Falls). Die Datenschutzvereinbarung stellte sicher, dass deutsches Datenschutzniveau bei der Verarbeitung in den USA gewährleistet werden sollte und dass auch vor Ort durch den Berliner Datenschutzbeauftragten Kontrollen vorgenommen werden könnten. Letzteres wurde durch Abstimmungen mit den amerikanischen Behörden sichergestellt.

Die Verarbeitung der Daten in den USA erfolgte ohne Beanstandung. Einzelne, bei dem Umfang des Projektes unvermeidliche Fehler wiesen nicht auf grundsätzliche Mängel hin. In einem einzigen Fall, bei dem die versagte Einwilligung des Datentransfers in die USA gleichwohl zu einer Datenübermittlung führte, kam es zu gerichtlichen Auseinandersetzungen[146], die schließlich mit einem Vergleich endeten.

Die Kooperation zwischen der DB und der Citibank endete am 31. März 1999 aus betriebswirtschaftlichen Gründen. Seither wird die BahnCard (wie bereits vor 1995) in Deutschland von der MSN Bertelsmann produziert. BahnCard und Kreditkarte wurden entkoppelt. Die seit Sommer 1998 laufende Abwicklung der Kooperation im Hinblick auf die Verarbeitung der Kundendaten wurde von uns in mehreren Gesprächen überprüft. Hierbei ergab sich kein Grund für eine Beanstandung. Ursprüngliche Bedenken, dass es technisch nicht möglich sein würde, die Passfotos derjenigen Kunden, die keine Visacard mehr haben wollten, aus dem Datenbestand der Citibank zu entfernen, erwiesen sich als verfehlt.

Das 3-S-Konzept

*Die DB möchte mit ihrem 3-S-Konzept **S**ervice, **S**icherheit und **S**auberkeit im Bahnhofsbereich verbessern. Dazu werden nacheinander die großen Personenbahnhöfe mit Videoanlagen ausgerüstet, die über fern-*

145 JB 1995, 3.1
146 Amtsgericht Kassel, Urteil v. 3. 11. 1998, Az.: 424 C 1260/98

gesteuerte Speed-Dome-Kameras verfügen und weite Bereiche des Bahnhofes erfassen. Sie werden über mehrere Monitore von den Mitarbeitern der DB in den 3-S-Zentralen beobachtet, aus denen der Einsatz der Mitarbeiter im Bahnhofsbereich koordiniert wird.

Bis zum Jahr 2001 sollen 46 derartige 3-S-Zentralen eingerichtet werden, darunter die Berliner Bahnhöfe Zoologischer Garten, Lehrter Bahnhof, Lichtenberg und Ostbahnhof. Da es sich bei der Videoüberwachung auf den Bahnhöfen der DB (mit Hauptsitz in Berlin) um eine Angelegenheit von überregionaler und zentraler Bedeutung handelt, haben wir exemplarisch den in der Entwicklung am weitesten fortgeschrittenen Ostbahnhof besichtigt und geprüft, ob bei der *Videoüberwachung* datenschutzkonform verfahren wird.

Auf der Grundlage unserer Position zur Videoüberwachung[147] haben wir bei Besichtigung des Ostbahnhofs empfohlen, die im Bahnhofsbereich bereits vorhandenen *Hinweise* zu verbessern. Da die zum Bahnhof führenden Zugänge und die unter der Hochbahntrasse entlangführende Straße, also öffentliche Straßenbereiche, ebenfalls von der Videoüberwachung betroffen sind, haben wir auch hier das Anbringen von deutlich sichtbaren Hinweisen empfohlen. Eine Aufklärung ist an den auf den Bahnsteigen befindlichen *Notrufsäulen* erforderlich. Von einer Gefahrenlage, die die Aufzeichnung von Bild und Wort rechtfertigt, ist bei Betätigung des Notrufknopfes durch den Betroffenen auszugehen.

Ein an die 3-S-Zentrale angrenzender verschlossener Raum wird vom *Bundesgrenzschutz* (BGS) genutzt und ist mit Monitoren, die ihrerseits an die Videoanlage des 3-S-Systems angeschlossen sind, ausgestattet. Entsprechend den Empfehlungen des Bundesbeauftragten für den Datenschutz[148] wurden die Arbeitsbereiche der Mitarbeiter der DB zur Erfüllung der bahneigenen Aufgaben einerseits und der Arbeitsbereich für die Mitarbeiter des BGS zur Erfüllung der bahnpolizeilichen Aufgaben andererseits getrennt voneinander gehalten, so dass eine optische und akustische Abschottung der Arbeitsbereiche voneinander gewährleistet ist. Auch die Auflage des BfD, dass die Bilder in der Leitzentrale abgeschaltet werden, wenn die Polizei selbst die Kamera führt, wird eingehalten.

Hinsichtlich des Mitarbeiterdatenschutzes haben wir uns davon überzeugt, dass eine Betriebsvereinbarung die Nutzung der Videoaufnahmen für Verhaltens- und Leistungskontrollen ausschließt.

Anprangernde Adressierung

Ein Vater beschwerte sich darüber, dass er von der DB einen Brief erhalten habe, der adressiert worden ist an den Erziehungsberechtigten eines Kindes, das ohne gültigen Fahrschein angetroffen worden war. Zusam-

147 vgl. 3.1
148 16. Tätigkeitsbericht 1995–1996, 12.4

men mit der Absenderangabe und dem Stempelaufdruck „Fahrpreisnacherhebung" sei jedem klar, dass es sich um eine Schwarzfahrt des Kindes handeln müsse.

In der Tat wird jedem, der mit dem Brief in Berührung kommt (z. B. andere Mitarbeiter der DB, Postboten, Nachbarn, Mitbewohner des Empfängers), offenbart, dass der Betroffene noch nicht mündig ist und es bei dem mit dem Brief mitzuteilenden Sachverhalt um etwas derart Schwerwiegendes geht, dass es den *Erziehungsberechtigten* zur Kenntnis gegeben werden soll. Diese Datenübermittlung ist nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG unzulässig, weil die Art der *Adressierung* nicht zur Wahrung berechtigter Interessen der DB (an der Durchsetzung einer Forderung) erforderlich ist und zudem das schutzwürdige Interesse von Minderjährigen an dem Ausschluss derartiger Übermittlungen überwiegt. Dies gilt insbesondere deshalb, weil die DB den tatsächlichen Erziehungsberechtigten entsprechend den melderechtlichen Bestimmungen durch eine Melderegisterauskunft bei der örtlich zuständigen Meldestelle erfragen kann. Die DB hat sich unserer Auffassung angeschlossen und das Verfahren bei Fahrpreisnacherhebungen entsprechend geändert. Im Adressfeld erscheint der Name des Minderjährigen nicht mehr, sondern allein der Name und die Anschrift des gesetzlichen Vertreters. Im Übrigen wird auf den Briefumschlägen auf den Stempelaufdruck „Fahrpreisnacherhebung" verzichtet und eine neutrale Absenderangabe verwendet.

Berliner Verkehrsbetriebe

Die Berliner Verkehrsbetriebe sind das größte deutsche Nahverkehrsunternehmen. Auch beim Datenschutz sollten sie die Vorreiterrolle spielen.

tick.et

Dass der Umgang mit Bargeld den Rationalisierungsbestrebungen im Zahlungsverkehr entgegensteht, zeigt der ungebrochene Drang zu elektronischen Zahlungsweisen und Selbstbedienungssystemen in der Kreditwirtschaft. Im Gegensatz zu elektronischem Geld erfordert die Handhabung von Bargeld nach wie vor zeit- und kostenverschlingende Handarbeit. Darüber hinaus entspricht der Umgang mit den anonymen Münzen und Geldscheinen nicht der hohen Bedeutung von Kundenbindung und innerbetrieblicher Transparenz.

Obwohl die *elektronische Geldbörse* in Berlin bisher nur eine geringe Verbreitung gefunden hat, soll dieses Kartenmodell jetzt den öffentlichen Nahverkehr revolutionieren: Die Berliner Verkehrsbetriebe (BVG) haben am 1. Oktober 1999 mit dem Feldversuch für das *elektronische Ticketing* begonnen. Auch die S-Bahn GmbH hat sich nach einigem Zögern inzwischen dem Feldversuch angeschlossen.

Die Teilnehmer am Feldversuch bekamen dabei eine kontaktlos wirkende Chipkarte, das *tick.et,* ausgehändigt. Damit wurde das Recht erworben, einen Monat lang im gesamten Tarifbereich zu fahren.

Zur Infrastruktur des Feldversuchs gehört eine Reihe von kundenbezogenen Geräten:

- Das gelbe tick.et start-Terminal dient dem Kunden zum Einchecken. Mit dem Vorbeiführen der Chipkarte an einem Kontaktfeld erfolgt eine – im Feldversuch noch fiktive, weil finanziell sich nicht auswirkende – Abbuchung eines Pauschalbetrages an ÖPNV-Einheiten, der auf einem Display angezeigt wird. Dies entspricht der Entwertung eines Fahrscheins. Die Eincheckdaten werden auf dem tick.et gespeichert.
- Das blaue tick.et stop-Terminal dient dem Kunden zum Auschecken. Hier erfolgt eine – ebenfalls noch fiktive – Rückbuchung, falls der Pauschalbetrag den tatsächlichen entfernungs- und zeitabhängigen Wert der Fahrt überschritten hat. Dabei werden die Eincheckdaten zur Berechnung herangezogen.
- Das weißgelbe tick.et box-Terminal dient der Ausgabe oder Aufladung von Karten sowie Zahlung mit Bargeld, GeldKarte oder ec-Karte (mit PIN-Eingabe).
- Das weiß-gelb-blaue tick.et tip-Terminal dient der Abfrage von Auskünften rund um das System sowie zum Restwert der Karten und zum Lesen der Logdatei auf der Karte, die die Angaben der letzten zwanzig Ein- oder Auscheckprozesse sowie der letzten drei Ladetransaktionen enthält.

Das Ein- und Auschecken führt in den Hintergrundsystemen zur kartenbezogenen Erfassung der einzelnen Fahrten. Ein Bezug zu den Eigentümern der Karten kann nicht hergestellt werden, so dass Befürchtungen, die ÖPNV-Nutzer könnten gläsern werden, nicht gerechtfertigt sind.

Die BVG hat sich von Anfang an um unsere Einbeziehung bemüht und erklärt, dass ohne die strikte Beachtung aller datenschutzrechtlichen Vorgaben das Projekt nicht durchgeführt werden könne.

Datenschutzrechtlich entstand eine Reihe von Einzelfragen, die von Teilnehmern sowie der Presse an uns herangetragen wurden.

Die mit dem Feldversuch zusammenhängenden personenbezogenen Datenerhebungen müssen auf der Grundlage einer *Einwilligung* erfolgen. Die Daten sind für die Planung von Bedeutung, beim Echtbetrieb selbst dagegen, wenn die Nutzung des elektronischen Ticketings für jeden BVG-Kunden obligatorisch ist, nicht mehr erforderlich. Zwar sind beim Feldversuch und Echtbetrieb unterschiedliche Maßstäbe zu setzen. Nichtsdestoweniger muss auch beim Feldversuch auf die Erforderlichkeit abgestellt werden. Daher dürften auch bei der Analyse der

Fahrgastströme und der Vorbereitung einer entfernungs- und zeitbezogenen Tarifierung nur anonyme Daten verarbeitet werden.

Bei Karten, die den allmählichen Verbrauch eines Guthabens ermöglichen und damit personenbezogene Daten für ein späteres Clearing überflüssig machen, stellt sich die Frage nach dem *Reklamationsmanagement.* Auch beim tick.et muss der Kunde die Möglichkeit haben, bei technischen Störungen den Nachweis zu erbringen, dass auf der Karte mehr ÖPNV-Einheiten abgebucht als tatsächlich verfahren wurden. Umgekehrt hat auch die BVG einen legitimen Anspruch darauf, Gegenbeweise vorzubringen, wenn eine technische Störung von Kunden behauptet wird. Dem Anonymitätsanspruch würde jedoch widersprechen, wenn Nachweisdaten zentral in den Hintergrundsystemen gesammelt würden. Stattdessen wird ein Weg gegangen, der auch bei der GeldKarte der deutschen Kreditinstitute üblich ist: Das Protokoll wird auf der Karte selbst geführt und steht somit in der alleinigen Verfügungsgewalt des Karteninhabers. Die Logdatei auf dem tick.et enthält die letzten zwanzig Ein- bzw. Auscheckтransaktionen und die drei letzten Ladevorgänge.

Jeder Kartennutzer sollte schnell und einfach den Inhalt der Karte auslesen können. Er muss ja vor Antritt einer Fahrt wissen, ob das gespeicherte Guthaben für diese Fahrt ausreichend ist oder sie noch in den Geltungszeitraum der Karte fällt. Es wäre unpraktikabel, wenn diese Auskünfte ausschließlich am tick.et tip-Terminal abgefragt werden könnten. Es ist daher geplant, den Kunden kleine *Chipkarten-Lesegeräte,* sog. Wallets, anzubieten, mit denen die Chipkarte ebenfalls ausgelesen werden kann. Solche Wallets haben die Größe eines Schlüsselanhängers (und können dafür auch verwendet werden). Die Verwendung solcher Wallets ist aber bei kontaktlosen Chipkarten bisher nicht möglich. Daher soll das tick.et auch mit einem Kontakt ausgestattet werden. Wir haben empfohlen, dies im Feldversuch bereits einzuführen.

Bei der Nutzung des tick.et muss der Kunde erfahren, ob das Einchecken erfolgreich stattgefunden hat. Anderenfalls würde er Gefahr laufen, als Schwarzfahrer ertappt zu werden. Diese Rückkopplung erfolgt durch eine *visuelle* und *akustische Anzeige.* Die akustische Anzeige eines erfolgreichen Eincheckens erfolgt mit einer diskreten Tonfolge, ein erfolgloses Einchecken wird dagegen mit einem auffälligen akustischen Alarm quittiert, der im weiten Umkreis der Terminals zu hören ist. Wir haben bereits frühzeitig darauf hingewiesen, dass eine *Prangerfunktion* durch die Signalisierung nicht entstehen dürfe, da ein erfolgloses Einchecken viele Gründe haben kann, die nicht nur in Versäumnissen des Kunden, sondern auch in technischen Problemen liegen können. Diese Hinweise wurden zwar akzeptiert. Missverständliche Äußerungen, durch die Signalisierung solle man sehen, wer zahlt und wer nicht, führten in der Presse allerdings zur Behauptung, das tick.et sei eine Maßnahme gegen Schwarzfahrer.

Ein solcher Effekt ergibt sich durch Chipkarteneinsatz nicht. Schwarzfahrer können nach wie vor ohne tick.et oder Benutzung des tick.et fahren. Wer sich jedoch einchecken will, dies ihm aber lautstark verwehrt wird, hat mit Sicherheit nicht schwarzfahren wollen. Wir haben empfohlen, dass die Lautstärke zurückgenommen und durch Hinweise auf die Bedeutung des Signals aufmerksam gemacht wird. Dem wurde gefolgt.

Die Testphase soll die erforderlichen Daten für die endgültige Einführung des elektronischen Tickets liefern. Das Projekt, das in ambitionierter Weise für den öffentlichen Nahverkehr wegweisend sein soll, soll in ebenso vorbildlicher Weise die Belange des Datenschutzes, vor allem in technischer Hinsicht (privacy enhancing technologies), berücksichtigten. Wir haben unsere Mitwirkung hierzu zugesagt.

Schwarzfahrer

In unserem letzten Jahresbericht hatten wir ausführlich dargestellt, wie die in Berlin ansässigen Verkehrsunternehmen mit den Daten von *Schwarzfahrern* und von solchen Personen umgehen, deren Personalien von dem tatsächlichen Schwarzfahrer missbraucht wurden[149]. Problematisch war die unterschiedslose Speicherung der Daten für die Dauer von zwei Jahren bei der BVG. Um der nach § 3 Abs. 4 BetriebeVO vorgesehenen Einzelfallbetrachtung Rechnung zu tragen, haben wir empfohlen, eine Stichtagsregelung einzuführen, nach der die Daten im Einzelfall nach einem Jahr, spätestens nach zwei Jahren gelöscht worden wären. Dem hat sich die BVG nicht angeschlossen. Sie macht aus Vereinfachungsgründen von der zweijährigen Speichermöglichkeit keinen Gebrauch mehr, sondern löscht die Daten bereits ein Jahr nach dem Vorfall.

Auch die Verfahrensweise bezüglich der *Namensmissbrauchsdatei* hat die BVG auf unsere Empfehlung hin geändert. So werden die Daten der vom Personalienmissbrauch betroffenen Personen nur mit deren Einwilligung gespeichert. Die BVG hat überdies zugesagt, die bislang ohne Einwilligung der Betroffenen gespeicherten Daten zu löschen, wenn nicht die Betroffenen ihre Einwilligung erteilen (§ 17 Abs. 3 Satz 2, 3 BlnDSG).

BVG zieht Personalausweis ein

Ein Fahrgast der BVG hat sich darüber beschwert, dass ein BVG-Mitarbeiter anlässlich einer Fahrkartenkontrolle den vorgezeigten Personalausweis nicht nur zur Überprüfung der Personalien angesehen, sondern eingezogen und erst zurückgegeben habe, nachdem die Kontrollen der übrigen Fahrgäste im Oberdeck des Busses abgeschlossen und die Kontrolleure zum Aussteigen bereit gewesen seien.

149 JB 1998, 3.3

Die BVG stimmte mit uns darin überein, dass das Kontrollpersonal der BVG nicht berechtigt ist, quasipolizeiliche Befugnisse gegenüber dem Kunden geltend zu machen. Dementsprechend wurde gegenüber dem BVG-Mitarbeiter die notwendige arbeitsrechtliche Maßnahme ergriffen. Um Wiederholungsfälle zu vermeiden, haben wir empfohlen, eine schriftliche Arbeitsanweisung für das *Vorgehen des Kontrollpersonals* herauszugeben, in der auch darauf hingewiesen wird, dass schon die Vorlage des Personalausweises nicht verlangt, sondern allenfalls erbeten werden darf. Diesen Anforderungen hat die BVG durch eine an das Kontrollpersonal gerichtete Mitteilung entsprochen. Danach ist das Personal nicht berechtigt, die *Vorlage des Ausweises* zu verlangen. Bei freiwilliger Vorlage dürfen nur die Personalien (Name, Anschrift) abgeschrieben werden, der Ausweis ist sodann unverzüglich zurückzugeben.

4.6.4 Sonstige Unternehmen

Der CityServer

Bei der Ausstellung InterGeo im September 1998 in Wiesbaden stellte der TeleInfo Verlag, der zuvor schon eine rechtlich umstrittene CD-ROM mit dem deutschen Telefonbuch veröffentlicht hatte[150]*, ein ehrgeiziges Projekt unter der Bezeichnung „CityServer" vor: Aufgrund von hoch aufgelösten digitalen Farbfotos, die mit einem in einem Kleinbus montierten mobilen Bildaufnahme- und Wiedergabesystem erstellt werden, sollte eine Bilddatenbank erstellt werden, in der sämtliche Liegenschaften in Städten über 20 000 Einwohner erfasst werden. Im Laufe der letzten Jahre wurden die größten Städte bereits erfasst, Berlin war im Frühjahr vergangenen Jahres an der Reihe. Die Bilddatenbank soll für einen erheblichen Betrag Unternehmen und öffentlichen Stellen zur Verfügung gestellt werden. Eine abgespeckte Version kam im vergangenen Jahr unter der Bezeichnung „Talk Show" auf den Markt. Dort sind Bilder mit geringer Auflösung und ohne Flächendeckung mit einem Telefonverzeichnis kombiniert.*

Die Ankündigung des CityServers hat sofort eine öffentliche Diskussion über die Zulässigkeit derartiger Unternehmen ausgelöst. Der Bundesbeauftragte für den Datenschutz erklärte in einer Presseinformation, das geschilderte Verfahren stelle eine neue Dimension von Datenmacht in privater Hand dar und sei nach der bestehenden Rechtslage nicht zulässig. Auf Betreiben des Verlags wurde dem Bundesbeauftragten im Wege einer einstweiligen Anordnung aufgegeben, es zu unterlassen, sich über die Unzulässigkeit des Vorhabens zu äußern. Eine derartige negative Feststellung könne erst nach sorgfältiger Prüfung der Sach- und Rechtslage erfolgen, die zum Zeitpunkt der Entscheidung gerade von dem zuständigen niedersächsischen Landesbe-

150 JB 1997, 4.7.2

auftragten vorgenommen wurde. Verboten wurde ihm auch die Äußerung, das Vorhaben der Firma könne auch kriminellen Aktivitäten Tür und Tor öffnen.

Im Mai 1999 legte der niedersächsische Datenschutzbeauftragte das Ergebnis seiner Prüfung vor. Danach verstoße das Vorhaben in der derzeit angebotenen Form nicht gegen das geltende Datenschutzrecht. Zwar handele es sich entgegen der Auffassung der Firma beim Erstellen und Vertreiben der *Häuser- und Gebäudedatenbank* um die Verarbeitung personenbezogener Daten. Die weitere Anwendung des Bundesdatenschutzgesetzes scheide aber aus, weil die Daten nicht in oder aus Dateien verarbeitet werden, insbesondere sei eine automatisierte Auswertung der Gebäudedatenbank nach Straße und Hausnummer nicht möglich. Diese Auffassung wurde auch später von der Rechtsprechung geteilt[151].

Ungeachtet der Zuständigkeit des niedersächsischen Datenschutzbeauftragten teilen wir diese Auffassung nicht. Zusätzlich zu den Aufnahmen werden bei dem Verfahren die *Geo-Koordinaten* des jeweiligen Kamerastandpunktes mit Hilfe von Satellitensignalen gespeichert. Unter Angabe dieser Koordinaten kann in der Datei ein bestimmtes Haus aufgefunden werden. Verfügt man über eine bestimmte Adresse, sind somit die Bilder auswertbar, wenn eine Zuordnung zwischen genauer Adresse und Geo-Koordinaten möglich ist. Zwar wurde uns anlässlich einer Präsentation des Systems versichert, Stadtpläne, mit denen sich die Geo-Koordinaten der Adressen ermitteln ließen, seien derzeit auf dem deutschen Markt nicht verfügbar. Dies trifft jedoch nicht zu: Zumindest für die Städte Berlin, Hamburg, Düsseldorf und München werden derart geo-referenzierte Stadtpläne sogar im Internet angeboten. Somit liegt die für die Geltung des Bundesdatenschutzgesetzes erforderliche Auswertbarkeit des Datenbestandes vor.

Ungeachtet der juristischen Auseinandersetzungen um die Geltung des Bundesdatenschutzgesetzes stellen derartige Projekte jedenfalls einen erheblichen Eingriff in die Persönlichkeitsrechte der Eigentümer und Mieter dar. Zwar hat der Bundesgerichtshof vor vielen Jahren entschieden, dass ein Eigentümer aufgrund seiner Eigentümerstellung das *Fotografieren seines Hauses* und die Verwertung der Aufnahmen nicht verhindern kann, solange der Fotograf nicht das Grundstück betritt[152]. Fraglich ist jedoch, ob dies noch gelten kann, wenn die Aufnahmen mit Hilfe der modernen Informationstechniken jeder denkbaren kommerziellen Zielsetzung dienen können. Ein Eingriff in die Persönlichkeitsrechte liegt insbesondere dann vor, wenn auf den Bildern neben dem

151 Landgericht Waldshut/Thiengen, Entscheidung vom 14. 10. 1999, Az.: 1 O 200/99; Verwaltungsgericht Karlsruhe, Beschluss vom 1. 12. 1999, Az.: 1 ZK 2911/99

152 BGH NJW 1971, 1359; 1998, 2251

Gebäude selbst Personen oder andere identifizierbare Gegenstände (Kfz, Hausinschriften, Gegenstände, die auf besonderen Wohlstand hinweisen) abgebildet sind.

Die Übermittlung der Daten durch die Veröffentlichung des CityServers ist damit zumindest dann unzulässig, wenn der Eigentümer oder Mieter des Hauses Widerspruch gegen die Veröffentlichung eingelegt hat. Das Unternehmen hat sich denn auch ohne Anerkennung einer Rechtspflicht bereit erklärt, Widersprüche von Betroffenen gegen die Aufnahme ihres Hauses in die Datenbank zu beachten. Allerdings verlangt das Unternehmen die Übersendung eines Fotos des entsprechenden Hauses, um die Löschung vornehmen zu können. Die Angabe der genauen Geo-Koordinaten des Gebäudes bzw. der Adresse müssten hierfür genügen.

Ähnliche Projekte gibt es bereits in anderen europäischen Ländern, u.a. in Frankreich, Finnland, den Niederlanden sowie der Schweiz. In Frankreich können diese Daten sogar über das normale Telefonverzeichnis (Page Blanche) im Internet abgerufen werden. Auch hier ist damit zu rechnen, dass der CityServer oder ein ähnliches Produkt künftig im Internet erreichbar ist.

Angesichts dieser Entwicklung hat die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation in einem gemeinsamen Standpunkt gefordert, dass die „nationale Gesetzgebung dem Betroffenen zumindest ein Widerspruchsrecht gegen die systematische Sammlung und Speicherung derartiger Bilddaten über seine Wohnumgebung für kommerzielle Zwecke einräumen“ sollte. Nach der Entschließung der Arbeitsgruppe gibt es „einen Unterschied zwischen einem einzelnen Bürger, der für private Zwecke Aufnahmen eines bestimmten Gebäudes macht, und einem Unternehmen, das systematisch Bilder aller Gebäude in einer Stadt für kommerzielle Zwecke sammelt. Insbesondere muss der Betroffene das Recht haben, einer Einstellung dieser Daten in das Internet oder ihrer Speicherung auf elektronischen Datenträgern (z. B. CD-ROM) jederzeit zu widersprechen“[153]. Sowohl die Erstellung derartiger Datenbanken als auch die Möglichkeit des Widerspruchs sollte daher bei der Novellierung des BDSG berücksichtigt werden.

BGH begrenzt Telefonmarketing

In zwei Urteilen[154] hat der BGH seine bisherige Rechtsprechung zum Telefonmarketing bestätigt und Telefonwerbung als „besonders schwer wiegende Beeinträchtigung der verfassungsrechtlich geschützten Privat-

153 Gemeinsamer Standpunkt der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation zum Datenschutz bei Gebäude-Bilddatenbanken, Anlagenband „Dokumente zum Datenschutz 1999“, Teil C

154 BGH v. 16. 3. 1999, Az.: XI ZR 76/98 und BGH v. 24. 3. 1999, Az.: IV ZR 90/98

sphäre" eingestuft, da sie ein „praktisch unkontrollierbares Eindringen in die Lebensgewohnheiten der Zielperson erlaube" und den Bürgern im häuslichen Bereich „Anpreisungen von Waren und Dienstleistungen zu Zeiten aufzwinge, die ausschließlich der Werbende bestimmt".

Es ist bereits gefestigte Rechtsprechung des BGH, dass Werbung per Telefon nur mit vorherigem Einverständnis des Betroffenen zulässig ist und ein solches Einverständnis nicht schon allein in der Aufnahme eines geschäftlichen Kontakts gesehen werden kann. Der BGH hat darüber hinaus jedoch klargestellt, dass die *Einwilligung* der Betroffenen in das Telefonmarketing nicht durch *allgemeine Geschäftsbedingungen* herbeigeführt werden darf. Auch ein bestehendes Vertragsverhältnis ist kein ausreichender Rechtfertigungsgrund für die Verwendung einer formularmäßigen Zustimmungsklausel zur Telefonwerbung. Die Klauseln wurden vom BGH insgesamt als „unangemessene Benachteiligung der Kunden" im Sinne von § 9 AGB-Gesetz eingestuft.

Datenpreisgabe beim ec-Lastschriftverfahren

Wir haben zahlreiche Beschwerden von Bürgern erhalten, die bei Bezahlung durch Einzugsermächtigung im ec-Lastschriftverfahren vom Kassenpersonal aufgefordert wurden, ihren Personalausweis vorzulegen. Zusätzlich wurden Name, Adresse und gelegentlich sogar die Personalausweisnummer der Kunden notiert. Viele Kunden werden durch eine solche Vorgehensweise überrascht, da ihnen die Tatsache, dass ihre Adressdaten von dem Unternehmen gespeichert werden sollen, erst nach Einlesen der ec-Karte mitgeteilt wird. Eine nachträgliche Stornierung der Kartenzahlung wird vom Kassenpersonal entweder verweigert oder ist mit erheblichen Schwierigkeiten verbunden.

Im Rahmen eines Vertragsverhältnisses dürfen nur die Daten des Betroffenen gespeichert werden, die für die Erfüllung des Vertrages erforderlich sind (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Hierzu zählt auch die Geltendmachung von Rechtsansprüchen zur Durchsetzung einer bestehenden Kaufpreisforderung. Das Notieren von Namen, Anschrift oder sogar der Personalausweisnummer ist jedoch – auch zur Absicherung der Geltendmachung der Kaufpreisforderung – nicht erforderlich.

Die vom Kunden zu unterschreibenden Belege bei der Bezahlung im *Lastschriftverfahren* enthalten regelmäßig die Ermächtigung der Bank, für den Fall der Nichteinlösung der Lastschrift dem Unternehmen Namen und aktuelle Anschrift des Kontoinhabers mitzuteilen. Daher ist zum Zwecke der Durchsetzung des Zahlungsanspruchs durch den Gläubiger nicht erforderlich, von vornherein Namen und Anschrift des Schuldners zu speichern. Denn es besteht aufgrund der Einwilligung die Möglichkeit, bei Nichteinlösung der Lastschrift die zur Verfolgung des Schuldners erforderlichen Daten bei der Schuldnerbank in Erfahrung zu bringen. Ebenso sehen die Händlerbedingungen der Kreditwirt-

schaft zum ec-Lastschriftverfahren vor, dass das Karten ausgebende Kreditinstitut dem Unternehmen Namen und Adresse des Karteninhabers auf Anfrage mitteilen wird, wenn die Lastschrift nicht eingelöst wurde oder der Karten-/Kontoinhaber der Belastung widersprochen hat, eine Sperrdateiabfrage erfolgt ist und eine wirksame Einwilligung des Karteninhabers in die Weitergabe seiner Daten vorliegt.

Da die Unternehmen bei Bezahlung im ec-Lastschriftverfahren dem Kunden gegenüber in Vorleistung treten, haben wir keine Bedenken dagegen, dass gegebenenfalls die Vorlage des Personalausweises verlangt wird, um zu überprüfen, ob der Käufer berechtigter Inhaber der ec-Karte ist. Ein Unterschriftenvergleich von Personalausweis und ec-Karte ist ausreichend, um einen Missbrauch der ec-Karte auszuschließen und den Kunden als rechtmäßigen ec-Karteninhaber zu identifizieren. Auf der Einzugsermächtigung darf dann nur noch festgehalten werden, dass eine solche Identitätsüberprüfung stattgefunden hat. Die Adresse oder sogar die Personalausweisnummer muss hierfür nicht notiert werden.

Die betroffenen Unternehmen haben sehr unterschiedlich reagiert. Leider blieb das Vorgehen eines großen Unternehmens, das nach unserem Hinweis sofort sämtliche Filialen benachrichtigte und entsprechende Anweisungen an das Kassenpersonal erteilte, die große Ausnahme. In den allermeisten Fällen war die Unternehmensleitung nicht bereit, sich unserer Rechtsauffassung anzuschließen.

Bußgeldbescheide im Lottoladen

Mitte des Jahres haben verschiedene Berliner Behörden, u. a. der Polizeipräsident in Berlin, die Beförderung und förmliche Zustellung von Bescheiden mit Postzustellungsurkunden auf einen privaten Postzustelldienst übertragen. Viele Bürger waren daher sehr erstaunt, als sie in ihrem Briefkasten eine Benachrichtigungskarte mit dem Hinweis fanden, dass sie den zugestellten Bußgeldbescheid in einem Lotto- bzw. Zigarrengeschäft abholen könnten. Das Erstaunen wich Empörung, als sie feststellten, dass oftmals die Wahrung des Postgeheimnisses seitens der Geschäftsinhaber sowie die datenschutzrechtlichen Bestimmungen nicht eingehalten wurden. So berichtete eine Bürgerin, die sich gegenüber einem Ladenbesitzer darüber beschwert hatte, dass er sämtliche Dokumente wie den Nachweis über die Aushändigung des Schriftstücks, den Personalausweis sowie das Schriftstück selbst offen auf der Ladentheke ausgebreitet hatte und in dem kleinen Geschäft der Diskretionsabstand nicht gewahrt sei, dieser hätte ihr entgegnet: „Warum beschweren Sie sich denn? Wenn Sie sich im Straßenverkehr ordnungsgemäß verhalten hätten, wären Sie jetzt auch nicht hier." In einem anderen Fall erkundigte sich ein Bürger nach der Aufbewahrung der Gebührenbescheide in dem Lottogeschäft und erhielt die Antwort, diese seien „in einem Stahlbehältnis" gelagert. Tatsächlich holte der Geschäftsinhaber

den Bußgeldbescheid des Petenten aus einer offenen Kiste, die sich in einem frei zugänglichen Regal hinter der Ladentheke befand, hervor. Weitere Petenten machten ähnliche Erfahrungen, als sie die Gebührenbescheide in den „Agenturstellen" abholen wollten.

Dies ist ein Beispiel dafür, dass die Liberalisierung des *Postdienstes* sowohl im Hinblick auf die Sicherung der Einhaltung des grundrechtlich geschützten Postgeheimnisses als auch Einhaltung der datenschutzrechtlichen Bestimmungen zahlreiche Probleme aufwirft. Im Zuge der *Privatisierung* der Post vergibt die Regulierungsbehörde für Telekommunikation und Post Lizenzen für die Briefzustelldienste an Privatunternehmen. Der private Zustelldienst, der von mehreren Berliner Bezirksämtern sowie vom Berliner Polizeipräsidenten mit der förmlichen Zustellung von Schriftstücken durch Postzustellungsurkunde beauftragt wurde, hat einen Agenturvertrag mit 23 Lotto- und Pressegeschäften in Berlin geschlossen. Soweit der Empfänger des behördlichen Schreibens nicht angetroffen wird, werden die Schreiben in den „Agenturstellen" aufbewahrt und an die Empfänger herausgegeben.

Eine förmliche Zustellung kann sowohl durch die Behörde selbst als auch durch die Post durch Zustellungsurkunde mittels eingeschriebenen Briefes erfolgen (§ 2 Abs. 1, §§ 3 und 4 Verwaltungszustellungsgesetz). Nach der Privatisierung der Post und der Aufhebung des *Zustellungsmonopols* muss der Begriff „Post" hierbei im Sinne eines Postzustelldienstes verstanden werden. Die Ausstellung der *Zustellungsurkunde* ist hoheitliches Handeln. Umstritten ist die Frage, ob nur die Zustellung des Bescheides selbst oder auch die Niederlegung des förmlich zuzustellenden Schriftstücks als hoheitliche Tätigkeit anzusehen ist. Nach der bisherigen Rechtsprechung des Bundesverwaltungsgerichts verliert die Sendung mit der Niederlegung bei der Post ihre Eigenschaft als Zustellbrief. Es erscheint fraglich, ob das Bundesverwaltungsgericht nach der Privatisierung der Post an dieser Auffassung festhalten wird, da nun die Niederlegung nicht mehr von einer staatlichen Einrichtung vorgenommen wird, so dass nunmehr möglicherweise nicht mit der gleichen Zuverlässigkeit gewährleistet ist, dass der Empfänger Kenntnis von dem zuzustellenden Schriftstück erhält, um seine Rechtsverfolgung oder Rechtsverteidigung danach ausrichten zu können.

Sieht man in der Niederlegung eine hoheitliche Aufgabe, so gilt: Hoheitliche Aufgaben dürfen von Privaten nur dann wahrgenommen werden, wenn sie entsprechend dem Umfang der Tätigkeit mit hoheitlichen Befugnissen ausgestattet wurden, also Beliehene sind. In § 33 Abs. 1 Satz 2 Postgesetz findet sich die ausdrückliche *Beleihung der Lizenznehmer,* die Briefzustelldienstleistungen, u. a. förmliche Zustellungen, erbringen. Diese Befugnis gilt jedoch nur für den Lizenznehmer selbst, nicht für etwaige Subunternehmer wie die vom privaten Briefzustelldienst beauftragten Presse- und Lottogeschäfte. Wird auch die Nie-

derlegung förmlich zuzustellender Schriftstücke als hoheitliche Tätigkeit angesehen, besitzen die Agenturvertragspartner des Lizenzunternehmens hierfür nicht die erforderlichen hoheitlichen Kompetenzen. Der Agenturvertrag wäre dann rechtswidrig.

In den vorliegenden Fällen wurden die Voraussetzungen des § 3 BlnDSG nicht eingehalten. Danach hat der Auftraggeber, d. h. hier der private Postzustelldienst, dafür Sorge zu tragen, dass die datenschutzrechtlichen Bestimmungen auch von dem durch ihn eingeschalteten Subunternehmer eingehalten werden. Der Auftraggeber hat zu gewähren, dass keine Informationen an unberechtigte Dritte weitergegeben werden. Obwohl sich in dem Agenturvertrag eine Regelung zum Datenschutz findet, wird die Einhaltung der datenschutzrechtlichen Bestimmungen durch den Auftraggeber ganz offensichtlich nicht ausreichend überwacht. Die geplante Beanstandung gegenüber dem Auftraggeber konnte nicht mehr erfolgen, da dieser zwischenzeitlich insolvent wurde und zukünftig wieder die Deutsche Post AG mit dem Transport der Behörden-Briefe beauftragt wird.

4.7 Europäischer und Internationaler Datenschutz

Die Safe-Harbor-Debatte

Vor dem Hintergrund der in Deutschland noch nicht umgesetzten, aber gleichwohl im Rahmen der Auslegung des Bundesdatenschutzgesetzes zu berücksichtigenden Bestimmungen zum internationalen Datenverkehr[155] kommt der Frage eine besondere Bedeutung zu, unter welchen Voraussetzungen die *Übermittlung personenbezogener Daten in die USA* zulässig ist. Da die USA im privaten Bereich über keine allgemeinen Datenschutzregelungen verfügen, besteht von Gesetzes wegen kein *angemessenes Datenschutzniveau* (Art. 25 Abs. 1 EU-Richtlinie). Dies führt dazu, dass Datentransfers einer besonderen Rechtfertigung bedürfen. Diese kann in der Einwilligung der betroffenen Personen, in der Erforderlichkeit für die Vertragsabwicklung, in der Wahrung „wichtiger öffentlicher" oder „lebenswichtiger" privater Interessen, in gerichtlichen Auseinandersetzungen oder in gesetzlichen Vorschriften bestehen. Häufig liegen diese relativ großzügigen Voraussetzungen gleichwohl nicht vor, etwa in den Fällen der Auftragsdatenverarbeitung, der Sammlung von Daten für Marketingzwecke oder der Einholung von Kreditauskünften.

Um den Datentransfer in die USA gleichwohl zu rechtfertigen, stellt die Richtlinie grundsätzlich zwei Instrumente zur Verfügung: Zum einen können die Partner, zwischen denen Informationen ausgetauscht werden sollen, *auf dem Vertragswege Garantien hinsichtlich des Schutzes der Privatsphäre,* der Grundrechte und der Grundfreiheiten der Perso-

155 JB 1998, 4.7

nen sowie hinsichtlich der Ausübung der damit verbunden Rechte vereinbaren (Art. 26 Abs. 2). Werden diese Verträge genehmigt, ist die Datenübermittlung zulässig. In der Vereinbarung zwischen der DB und der deutschen bzw. amerikanischen Citibank ist dieser Weg beschritten worden[156]. Eine internationale Debatte über die Erarbeitung von *„Model-Contracts“* will diese Möglichkeit nutzen[157].

Dieser Weg wird für eine Vielzahl von Fällen nicht als erstrebenswert angesehen. Andererseits besteht derzeit in den politischen Gremien der USA offensichtlich keine Neigung, eine „Omnibus“-Gesetzgebung zum Datenschutz in die Wege zu leiten. Vielmehr will man die bisherige Politik, einen Bereich nach dem anderen durch Spezialgesetze zu regulieren (Kreditinformationen, Datenverarbeitung bei Banken, medizinische Daten bis hin zur Datenverarbeitung in Videotheken), fortsetzen. Für alle anderen Anwendungen möchte man den zweiten Weg einschlagen, den die Richtlinie vorsieht. Die Europäische Kommission kann nach Zustimmung der Regierungsvertreter, die sich in einem Ausschuss nach Art. 31 der EU-Richtlinie regelmäßig abstimmen, feststellen, dass aufgrund internationaler Verpflichtungen, die der betreffende Staat nach Verhandlungen mit der Kommission eingegangen ist, ein angemessenes Schutzniveau gewährleistet ist. Das US-Handelsministerium hat unter der Bezeichnung *„Safe-Harbor-Principles“* einen Entwurf derartiger Verpflichtungen vorgelegt, nach denen ein Unternehmen, das sich ihnen unterwirft, gleichsam in einem sicheren Datenschutzhafen landet.

Die das ganze Jahr über zwischen den USA und der Europäischen Kommission geführten Verhandlungen haben bis Ende 1999 noch zu keinem endgültigen Ergebnis geführt. In ihrer letzten Sitzung im Jahr 1999 hat die Arbeitsgruppe nach Art. 29 der Richtlinie bedauert, dass ihre Einwände beim letzten Stand der amerikanischen Dokumente noch nicht berücksichtigt sind. Diese betreffen vor allem die Frage des Informationszugangs sowie der Durchsetzung der Datenschutzregeln. Auch der Ausschuss nach Art. 31 hält die Vereinbarung nicht für entscheidungsreif.

Damit bleibt es bis auf weiteres dabei, dass eine richtlinienkonforme Übermittlung personenbezogener Daten nur auf der Grundlage von Einzelverträgen mit dem amerikanischen Partner möglich ist, wenn nicht die allgemeinen Voraussetzungen vorliegen. Auch in diesen Fällen ist allerdings zu gewährleisten, dass bei der Verarbeitung der Daten in den USA die schutzwürdigen Belange der Betroffenen sichergestellt werden.

---

156 vgl. 4.6.3
157 vgl. 6.4

4.7

Arbeitsgruppe Internationaler Datenverkehr

Bereits im Jahr 1989, als die Aufgaben der Aufsichtsbehörde noch von der Senatsverwaltung für Inneres wahrgenommen wurden, hat die Konferenz der Obersten Aufsichtsbehörden („Düsseldorfer Kreis") eine Arbeitsgruppe „Internationaler Datenverkehr" unter dem Vorsitz Berlins gegründet. Diese Arbeitsgruppe hat 1993 eine „Checkliste" zur Gewährleistung des Datenschutzes beim grenzüberschreitenden Verkehr mit personenbezogenen Daten durch ein Vertragsmodell vorgelegt, das nicht ohne Einfluss auf den BahnCard-Vertrag war. Die Arbeit wurde vom Berliner Datenschutzbeauftragten kontinuierlich fortgesetzt. Sie zeigt, dass die datenschutzrechtliche Bewertung internationaler Datenflüsse schwierige Rechtsfragen aufwirft.

> *Ein großer Anbieter von Online-Diensten betreibt nicht nur den Server für sein weltweites Internetangebot in den USA; dort werden auch sämtliche Kundendaten verarbeitet. Das deutsche Tochterunternehmen nimmt die Daten der Kunden nur entgegen und stellt sie in den in den USA geführten Datenbestand ein. Änderungen im Datenbestand aufgrund von Telefonaten werden von Call-Centern vorgenommen, die auch in anderen europäischen oder außereuropäischen Staaten betrieben werden.*

Bei derartigen Fallkonstellationen ist bereits die Feststellung schwierig, welches Recht anzuwenden ist. Das bisherige deutsche Datenschutzrecht lässt diese Frage offen. Aus dem Regelungszusammenhang, insbesondere in Verbindung mit den Zuständigkeitsvorschriften des Verwaltungsverfahrensgesetzes (§ 3), ergibt sich jedoch, dass deutsches Recht immer dann anzuwenden ist, wenn die Datenverarbeitung in Deutschland stattfindet. Eine Erstreckung des deutschen Rechts auf Daten, die im Ausland verarbeitet werden, ergibt sich nicht von Gesetzes wegen, sondern erst dann, wenn der Datenexporteur im Hinblick auf die Wahrung schutzwürdiger Belange der Betroffenen (§ 28 Abs. 1 Satz 1 Ziff. 2 BDSG) einen Vertrag mit dem ausländischen Partner schließt, in dem die Geltung des deutschen Rechts vereinbart wird (wie z. B. beim *BahnCard-Vertrag*), oder wenn das ausländische Unternehmen eine unmittelbare Vereinbarung mit dem Betroffenen eingeht.

Die Richtlinie verändert diese Situation. In allen Fällen, in denen die speichernde Stelle eine Niederlassung im Inland unterhält, bleibt es zwar bei der Geltung des nationalen, also des deutschen Rechtes. Nach der Richtlinie soll sich das nationale Recht aber auch auf alle Verarbeitungen personenbezogener Daten erstrecken, die von einem Unternehmen durchgeführt werden, das in einem *Drittland* außerhalb der Europäischen Union seinen Sitz hat (z. B. USA), die Daten dort verarbeitet, aber für die Verarbeitung auf „automatisierte oder nicht-automatisierte Mittel" zurückgreift, die in einem europäischen Land gelegen sind. Daraus folgt, dass deutsches Recht künftig immer dann anzuwenden sein wird, wenn US-Unternehmen Daten zwar in den USA verarbeiten,

dabei aber Datenverarbeitungsgeräte verwendet werden, die sich im Inland befinden. Auf die Nationalität der betroffenen Personen kommt es nicht an.

Für den vorliegenden Fall bedeutet das: Für die Erhebung der Kundendaten in Deutschland findet deutsches Recht Anwendung, ebenso für die Übermittlung in die USA. Die Erstreckung des deutschen Rechts auf die Verarbeitung der Daten in den USA muss eigens vereinbart werden – sei es durch Vertrag des Tochterunternehmens mit der Mutter, sei es durch unmittelbare Vereinbarung mit den Kunden. Für die Daten, die bei der Nutzung des Internet in den USA anfallen, gilt nach der Richtlinie hingegen unmittelbar deutsches Recht, wenn automatisierte „Mittel" des Anbieters in Deutschland, etwa Einwahlknoten genutzt werden, auch wenn die Daten dort nicht selbst verarbeitet werden. Allein die Tatsache, dass für die Internetnutzung ein (privater) PC in Deutschland verwendet wird, kann dagegen nicht ausreichen. Für Datenveränderungen, die z. B. von einem irischen *Call-Center* auf dem amerikanischen Datenbestand vorgenommen werden, gilt irisches Recht, wenn nichts anderes vereinbart ist.

Unklar bleibt nach den Bestimmungen der Richtlinie, welches Recht anzuwenden ist, wenn das Daten verarbeitende Unternehmen seinen Sitz in einem anderen Staat der EU hat, aber nicht über eine Niederlassung in Deutschland verfügt. Nach der Logik des Europarechtes muss dabei das *Recht des europäischen Sitzlandes* gelten, mit der für die Aufsichtsbehörden künftig nicht ganz einfach zu bewältigenden Folge, dass auf bestimmte Datenverarbeitungsvorgänge im Inland das Recht eines anderen europäischen Staates anzuwenden ist.

Aus dieser Situation, die durch die offene Frage der Direktwirkung der Richtlinie[158] noch erschwert wird, ergibt sich die dringende Empfehlung, in allen diesen Fällen das deutsche Recht vertraglich zu vereinbaren.

> *In Krankenhäusern und anderen medizinischen Einrichtungen werden zunehmend medizinische Geräte eingesetzt, deren Datenverarbeitungsfunktionen bei den Herstellern nur aus der Ferne gewartet werden. Für amerikanische Geräte bedeutet dies, dass ein Zugriff auf medizinische Daten und damit eine Datenübermittlung in die USA möglich ist.*

Die Frage, unter welchen Voraussetzungen *Auftragsdatenverarbeitung bei medizinischen Daten* möglich ist, ist für sich schon ein Problem[159]. Es wird dann bei der bestehenden Rechtslage kaum mehr lösbar, wenn der Datenzugriff aus einem Land erfolgen soll, in dem keine Datenschutzgesetze existieren. Dieses das Krankenhausmanagement zunehmend

158 vgl. oben

159 z. B. Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Betreuungseinrichtungen v. 17./18. 4. 1997

bedrängende Problem lässt sich derzeit nur dadurch lösen, dass auch bei Fernwartung, durch technisch-organisatorische Maßnahmen, der Zugriff auf die Daten selbst verwehrt wird. Auf diese Weise werden keine personenbezogenen Daten ins Ausland übermittelt. Die entsprechenden Instrumente hierzu zu entwickeln ist eines der wichtigen Themen für die Entwicklung von Privacy Enhancing Technologies.

Ein deutsches Unternehmen hat eine Tochtergesellschaft in einem benachbarten Land, das nicht der EU angehört. Die Daten des Tochterunternehmens (Personaldaten, Lieferantendaten, Kundendaten) sollen in dem Rechenzentrum des Mutterunternehmens in Deutschland verarbeitet werden.

Auch hier nutzt das ausländische Tochterunternehmen Informationstechnik, die in Deutschland gelegen ist. Nach der Richtlinie ist deutsches Recht anzuwenden, was sich ohnehin aus dem geltenden deutschen Recht bereits ergibt. Sollte dem ausländischen Tochterunternehmen der *Zugriff auf Daten der deutschen Muttergesellschaft* gestattet werden, was bei Lieferanten- und Kundendaten nahe liegt, liegt beim Abruf im Einzelfall eine Datenübermittlung in ein Drittland vor. Handelt es sich wie im vorliegenden Fall um ein Land, bei dem ein ausreichendes Datenschutzniveau noch nicht festgestellt ist, ist die geradezu zwingende Lösung, dass ausländische Tochterunternehmen in vollem Umfang dem deutschen Datenschutzrecht durch Vertrag unterstellt werden müssen.

Ein Mitarbeiter einer Berliner Verwaltung möchte die dort vereinbarte Regelung zur Heimarbeit nutzen. Hierfür ist allerdings die Verarbeitung von personenbezogenen Daten mit Hilfe eines mobilen Datenverarbeitungsgerätes (Laptop) erforderlich. Sein Problem ist, dass er die Heimarbeit in den Niederlanden verrichten möchte.

Das Besondere an diesem Fall ist, dass die Herrschaft über die personenbezogenen Daten den Bereich der behördlichen Zuständigkeit nicht verlässt. Die Heimarbeitsvereinbarung führt dazu, dass der häusliche Arbeitsplatz dienstlichen Charakter hat und es mithin nicht zu einer Datenübermittlung ins Ausland, sondern lediglich zu einer Datennutzung im Ausland kommt. In diesem Fall liegt es nahe, die Regelungen über die Datenübermittlung ins Ausland nicht anzuwenden, sondern entsprechend den Regelungen im *internationalen Arbeitsrecht* von der ausschließlichen Geltung des deutschen Rechtes auszugehen (*„Käseglockentheorie“*). Diese Auffassung teilte auch die niederländische Datenschutzbehörde Registratiekamer. Diese wies allerdings darauf hin, dass hinsichtlich der technisch-organisatorischen Maßnahmen bei dieser Fallkonstellation *niederländisches Recht anzuwenden* ist, da dieses unabhängig von der Art der verarbeiteten Daten für alle informationstechnischen Geräte gilt, die sich in den Niederlanden befinden.

4.8 Organisation und Technik

4.8.1 Verschlüsselung im Berliner Landesnetz – eine unendliche Geschichte?

Es war zu Beginn des Jahres 1994, als bei den Planungen zum Berliner Landesnetz zwei Datenschützer schon beim ersten Treffen darauf hinwiesen, dass personenbezogene Daten bei der Übertragung vor unbefugter, auch unabsichtlicher, Kenntnisnahme, Veränderung oder Löschung zu bewahren sind. So verging Jahr um Jahr, Kabel um Kabel wurde gezogen, eine um die andere Verwaltung wurde an das Landesnetz angeschlossen und es wurden fleißig Daten übertragen. Unsere regelmäßigen Hinweise auf ein *Verschlüsselungsgebot* wurden zwar kopfnickend zur Kenntnis genommen, jedoch verschlüsselt wurden die personenbezogenen Daten nicht. So kam dann das Jahr 1999. Sollte nun etwa alles anders werden?

Erst jetzt erfolgte eine Ausschreibung für ein verfahrenübergreifendes und anwendungsunabhängiges Verschlüsselungsprodukt für das Berliner Landesnetz durch den Landesbetrieb für Informationstechnik (LIT). Im Anschluss an die Ausschreibung wurden zwei Produkte ausgiebig getestet.

Das cryptSSL-Verfahren der Firma Giesecke & Devrient basiert auf einem symmetrischen Verschlüsselungsverfahren (die Ver- und Entschlüsselung von Daten basiert hierbei auf ein und demselben Schlüssel) mit einer Schlüssellänge von 128 Bit. Die Voraussetzungen für eine genügend sichere Datenübertragung wären damit gegeben. Leider konnte dieses Produkt nicht erfolgreich mit dem Berliner Haushaltsverfahren ProFiskal und dem auf SAP R/3 basierenden Personalverfahren IPV getestet werden.

Den Zuschlag in dem Ausschreibungsverfahren erhielt das Produkt SunScreen SKIP der Firma Sun Microsystems. Dieses Verfahren basiert auf dem wohl bekanntesten symmetrischen Verschlüsselungsverfahren *DES* (Data Encryption Standard) und konnte erfolgreich mit den Berliner Großverfahren getestet werden. Der DES-Algorithmus arbeitet standardmäßig mit einer Schlüssellänge von 56 Bit. Das Produkt SunScreen SKIP unterliegt jedoch den amerikanischen Exportbeschränkungen für Waffenlieferungen und darf daher in Deutschland nur mit einer Schlüssellänge von 40 Bit eingesetzt werden, eine Schlüssellänge, die einem Brute-Force-Angriff (computergestütztes Ausprobieren aller möglichen Schlüssel) mit leistungsstarken Rechnern nur kurze Zeit standhält: Ein Rechner, der für die Ermittlung eines 56-Bit-Schlüssels im Mittel 30 Tage benötigt, errechnet einen 40-Bit-Schlüssel im Mittel in 40 Sekunden. Ein Antrag auf eine Ausnahmegenehmigung für eine Schlüssellänge von 56 Bit ist zwar möglich, jedoch dauert die Bewilligung einerseits 8 – 12 Monate. Andererseits werden die die Sicherheit

erhöhenden 16 Bit mehr an Schlüssellänge bei der *NSA* (National Security Agency) in den USA hinterlegt, so dass zumindest dieser Nachrichtendienst Zugang zu den Daten erhalten kann.

Auch das Bundesamt für Sicherheit in der Informationstechnik hat bereits 1994 darauf hingewiesen, dass selbst eine Schlüssellänge von 56 Bit angesichts der Entwicklung schnellerer Rechner für künftige Verfahren nicht mehr zu empfehlen ist und stattdessen auf Verfahren wie z. B. *Triple-DES* (dreimaliges Anwenden des DES-Algorithmus mit zwei verschiedenen Schlüsseln) mit der Schlüssellänge von 112 Bit zurückgegriffen werden sollte.

Gleichwohl haben wir uns bisher darauf beschränkt, für die gängigen personenbezogenen Anwendungen eine 56-Bit-Verschlüsselung zu fordern, weil angenommen wird, dass die im Berliner Landesnetz zu übertragenen Daten keine solche Begehrlichkeiten wecken, dass von Angreifern der notwendige Aufwand betrieben wird, um diesen Schlüssel anzugreifen.

Diese Annahmen werden zunehmend brüchig und können angesichts der technischen Entwicklung nur noch für beschränkte Zeit als gültig angesehen werden. So wurde mittlerweile bekannt, dass Daten über Empfänger sozialer Transferleistungen bei Unternehmen hohe Begehrlichkeiten wecken, die auf die Beschaffung von Daten über die Kreditwürdigkeit spezialisiert sind. Ferner ist bekannt, dass Wirtschaftsspionage ein wesentliches Motiv zur „Überwachung“ des Datenverkehrs darstellt. Daher halten wir symmetrische Verfahren nur für zukunftssicher, wenn die Schlüssellänge mindestens 112 oder 128 Bit beträgt. Mit 56-Bit-Verschlüsselungen dürfte man professionellen Angriffen nicht mehr lange entgegenwirken können.

Die 40-Bit-Verschlüsselung hilft also nur gegen die unbeabsichtigte und beiläufige Kenntnisnahme des Datenverkehrs. Sensible Daten, die die Begehrlichkeit Dritter wecken, können damit nicht wirksam geschützt werden. Aus diesem Grunde hat es uns überrascht, dass der Landesbetrieb für Informationstechnik dieses Verschlüsselungsverfahren im Ergebnis einer Ausschreibung überhaupt erprobt hat.

Mittlerweile wird ein deutsches Verschlüsselungsprodukt für den Einsatz im Berliner Landesnetz getestet. Dieses Produkt kann mit verschiedenen symmetrischen Verschlüsselungsalgorithmen und einer Schlüssellänge von bis zu 168 Bit arbeiten. Der Erprobungsbericht zu diesem Test liegt vor und endet mit dem Satz:

> *„Das Produkt SafeGuard VPN wird für den Einsatz im Land Berlin empfohlen. Der LIT wird auf dieser Grundlage einen Infrastrukturdienst VPN aufbauen, mit dem eine authentisierte und verschlüsselte Kommunikation sowohl innerhalb des Berliner Landesnetzes (MAN) als auch über Anbindungen von Fremdnetzen realisiert wird.“*

Nun scheint die Geschichte doch noch ein gutes Ende zu nehmen.

4.8.2 MS-Windows NT

Das Betriebssystem *MS-Windows NT* ist sehr verbreitet. Grundsätzlich bietet Windows NT eine recht gute Abdeckung der Sicherheitsanforderungen. Mit der Auslieferung an den Nutzer ist das Betriebssystem jedoch auf einen möglichst unbeschränkten Zugriff ausgelegt. Dies bedeutet, dass der Nutzer das Betriebssystem erst an seine Sicherheitsbedürfnisse anpassen muss. Hier können Sicherheitsprobleme entstehen, wenn der Anwender z.B nicht über ausreichende Fachkenntnisse verfügt. Zudem werden immer wieder Sicherheitslücken in Windows NT entdeckt.

Die Risiken bestehen in:

- Ausspähen, Manipulation und Missbrauch von Informationen,
- Social Engineering oder andere Passwortattacken,
- Abhören von Netzwerkleitungen z. B. durch den Einsatz von Sniffern,
- Sabotage des Informationssystems vor Ort oder über Kommunikationsnetze.

Vor der Implementierung müssen Entscheidungen z. B. zum Netzaufbau – *Domänenmodell* mit evtl. einzurichtenden Vertrauensstellungen – oder die Einrichtung von Gruppen und Nutzern mit entsprechender Rechtevergabe auf Objekte oder Verzeichnisse bzw. Dateien getroffen werden.

Vor dem Starten des Betriebssystems kann durch Aktivierung des *BIOS-Passwortes* – nur nach Eingabe dieses Passwortes startet der Rechner – die erste Sicherheitsvorkehrung getroffen werden.

Geeignete Maßnahmen, die das Starten eines anderen Betriebssystems oder den zusätzlichen Einsatz von Manipulationsprogrammen, die die Sicherheitseinstellungen des Betriebssystems aushebeln, verhindern, sind:

- die Sicherung des Rechner-Gehäuses und der Schnittstellen für externe Geräte, z. B. durch Verplombung,
- die Vermeidung der Installation weiterer Betriebssysteme,
- der Schutz der Disketten-, CD-ROM- oder anderer externer Speichermedienlaufwerke, die ein Booten von selbigen zulassen, z. B. durch Laufwerksschlösser,
- das Setzen des Boot-Timeouts auf 0 Sekunden.

Als Dateisystem sollte ausschließlich *NTFS* eingesetzt werden, da hiermit die „erweiterten“ Sicherheitsfunktionen von Windows NT aktiviert werden, die den Zugriff auf Dateien und Verzeichnisse über die Zugriffskontrollliste steuern.

4.8.2

Das Betriebssystem kann aufgrund seines Sicherheitssystems bei entsprechender Ausgestaltung der vorgesehenen Identifizierung und Authentifizierung, verbunden mit der Einrichtung von nutzerspezifischen Zugriffsrechten bzw. Berechtigungen, ein entsprechendes Sicherheitsniveau bieten. Diese Einstellungen sind bei Berücksichtigung der Möglichkeit z. B. des expliziten Durchreichens von Login-Anforderungen an weitere Windows NT-Systeme sensibel zu vergeben. Rechte sollten zuerst so weit wie möglich eingeschränkt werden, um diese z. B. bei speziellen Anforderungen zu erweitern.

Hierbei sind jedoch für den Einsatz von *Identifizierungs- und Authentifizierungsmechanismen* dem Schutzzweck entsprechende Mindestanforderungen zu stellen.

Dies bezieht sich insbesondere auf Festlegungen zur Passwortgestaltung, wie z. B.:

- Mindestlänge (≥ 6 Zeichen), der Administrator mindestens 10 Zeichen,
- alphanumerischer Zeichenmix,
- zwangsweiser zyklischer Passwortwechsel,
- Zulassen bereits benutzter Passwörter erst nach mehreren Wechseln[160].

Nicht allein die Passwortgestaltung ist wichtig, sondern auch die der Benutzerkonten.

Folgende Eigenschaften sollten aktiviert werden:

- Der Nutzer muss sein Passwort ändern können, damit ein regelmäßiger Wechsel erfolgen kann.
- Das so genannte Einstiegspasswort, welches der Administrator vergibt, muss sofort gewechselt werden können.
- Das Konto sollte nach mehrmaligen Fehlversuchen gesperrt werden, damit evtl. Einbruchsversuche unterbunden werden können.

Mit dem Benutzerprofileditor und Anmeldeskripten können weitere Einschränkungen für den Nutzer vorgenommen werden.

Die Zugriffsrechte auf zu vergebende Ressourcen werden mit den folgenden Tools vergeben:

- Datei-Manager,
- Druck-Manager,
- Benutzermanager für Domänen und
- Benutzerprofileditor.

---

[160] BlnBDA: Empfehlungen für die Vergabe von Passwörtern, Materialien zum Datenschutz Nr. 25, 2. Auflage 1999, Anlage 2

Weil immer wieder neue Sicherheitslöcher entdeckt werden, sollten die angebotenen *Servicepacks bzw. Patches* regelmäßig installiert werden, da hierdurch entdeckte Sicherheitslücken des Betriebssystems geschlossen werden. Da die Installation von diesen „Lückenfüllern" jedoch teilweise die Rechte wieder in den unsicheren Erstinstallationszustand zurücksetzt, muss eine erneute Kontrolle aller bis dahin durchgeführten Rechtevergaben erfolgen.

Vordefinierte Konten wie z. B. „Gast" sollten deaktiviert bzw. überprüft werden, ob hier zu viele Rechte vergeben wurden. Der *„Administrator"-Account* sollte umbenannt werden, da ansonsten bei Hackversuchen ein erhöhtes Sicherheitsrisiko – etwa durch eine unbegrenzte Anzahl von Anmeldeversuchen – besteht. Auch sollte z. B. die *Gruppe „Jeder"* gelöscht bzw. deren Rechte so weit wie möglich eingeschränkt werden, da bei Zugriffsberechtigung dieser Gruppe auf ein Objekt auch Nutzer ohne Account darauf zugreifen können. Sollte dies zu Problemen führen, so sollte zumindest der Account „Jeder" durch die zugelassenen Benutzer ersetzt werden.

Darüber hinaus sollten die eingestellten Dienste, die nicht benötigt werden, deaktiviert und der Zugriff auf die Registry und das Systemverzeichnis (nur lesender Zugriff) eingeschränkt werden:

Die *Protokollierung* sollte genutzt werden, da hiermit Einbruchsversuche in das System festgestellt werden können. Hierfür sind jedoch vorherige sorgfältige Überlegungen notwendig, da eine ausufernde Protokollierung sicherheitsrelevante Ereignisse nicht mehr kenntlich macht oder nur zur vorzeitigen Füllung der vorgesehenen Speicherkapazitäten führt.

Durch den Einsatz von Zusatzprodukten können die *Laufwerke und Schnittstellen des Rechners* relativ sicher geschützt werden. Dies ist gerade beim Diskettenlaufwerk empfehlenswert, da ansonsten ein großes Gefährdungspotential für das IT-System bestehen würde. So können unbemerkt Kopien von Datenbeständen gezogen werden, die sich jeder weiteren Kontrolle entziehen. Auch das unbemerkte Einspielen von Tools ist möglich, was zu Manipulationen von Programmen oder Daten genutzt werden könnte.

Die Hard- und Softwarekonfiguration sollte sorgfältig dokumentiert und ständig aktualisiert werden. Dies gilt natürlich auch für die eingestellten Sicherheitsmaßnahmen. Eine ausführliche *Dokumentation* kann im Schadensfall bei der Behebung verschiedenster Fehler sehr zur Unterstützung beitragen.

Ein guter Systemadministrator sollte typische Hacker-Angriffstechniken kennen, damit er sich gut gegen diese schützen kann. Z. B. kann das Ausspähprogramm „L0phtCrack" durch Auslesen der Sicherheitskontenbank eines NT-Systems Passwörter ausspähen, dies setzt jedoch eine gültige Kennung und Passwörter in Verbindung mit Administratorenrechten voraus.

4.8.2

Folgende kostenlose Newsletter bzw. Internetseiten geben den Systemadministratoren weitere Hinweise:

- Microsoft Security Bulletin unter http://msdn.microsoft.com/workshop/essentials/mail.asp,
- PC Magazin News zu Windows NT unter http://www.pc-magazin.de/mailing/default.htm,
- SecurityFinder unter http://www.securityfinder.com,
- http://www.microsoft.com/security,
- http://www.trustedsystems.com/NSAGuide.htm,
- http://www.ntbugtraq.com/archives/ntbugtraq.html,
- http://www.ntshop.net/,
- http://www.it.kth.se/„Schlangenlinie“rom/ntsecindex.html,
- http://www.topsecret.net/NT/index.htm,
- http://www.ntresearch.com/ntsec.html,
- http://www.ntfaq.com,
- http://ntsecurity.ntadvice.com.

5. Telekommunikation und Medien

5.1 Telekommunikationsnetze

Europäische Telekommunikations-Richtlinie

Die Europäische Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (früher ISDN-Richtlinie)[161] bestimmt in Art. 15 Abs. 1 eine Umsetzungsfrist für die Mitgliedstaaten bis zum 24. Oktober 1998. Die erforderliche Anpassung der *Telekommunikationsdienstunternehmen-Datenschutzverordnung* (TDSV)[162] ist im zurückliegenden Berichtszeitraum wiederum nicht gelungen. Allerdings hat das Bundeswirtschaftsministerium in diesem Zeitraum einen Referentenentwurf für die Neufassung der TDSV (Stand 21. Oktober 1999) vorgelegt.

Bedauerlicherweise ist aus dem vorliegenden Entwurf keine Tendenz zur zukunftsweisenden Novellierung des Telekommunikationsdatenschutzrechts durch Einführung datenschutzfreundlicher Technologien zu verzeichnen. Der Entwurf enthält dagegen an zahlreichen Punkten sogar Verschlechterungen des Datenschutzniveaus gegenüber der jetzt gültigen TDSV[163]:

Der Verordnungsgeber hat wiederum die Möglichkeit ungenutzt gelassen, die bereits im Bereich der Tele- und Mediendienste niedergelegten Grundsätze der *datensparsamen Gestaltung von Diensten* auch auf den Telekommunikationsbereich auszuweiten, etwa durch Rahmenbedingungen für den Einsatz datenschutzfreundlicher Technologien und das Angebot einer *anonymen* bzw. *pseudonymen* Nutzung. Insbesondere ist die von uns mehrfach geforderte Einführung des „holländischen Modells", bei dem der angerufene Teilnehmer ein Wahlrecht erhält, ob seine Telefonnummer auf *Einzelverbindungsnachweisen* der Anrufer ausgewiesen wird[164], wiederum unterblieben. Dies ist insbesondere im Hinblick darauf bedauerlich, dass die ISDN-Richtlinie die Mitgliedstaaten verpflichtet, darauf hinzuwirken, dass für öffentlich zugängliche Telekommunikationsdienste Funktionen entwickelt werden, die den anonymen Zugang zu diesen Diensten ermöglichen (Erwägungsgrund 19 der Richtlinie).

Auch in verschiedenen anderen Bereichen enthält der Entwurf Regelungen, die gegenüber den Bestimmungen der jetzt gültigen TDSV zu einer Absenkung des Datenschutzniveaus im Bereich der Telekommunikation führen würden:

---

161 ABlEG L 24/1
162 BGBl. I 1996, S. 982 ff.
163 vgl. auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation", Anlagenband „Dokumente zum Datenschutz 1999", Teil A I
164 vgl. zuletzt JB 1998, 5.2

5.1

Nach der gegenwärtig geltenden Fassung der TDSV (§ 6 Abs. 4) hat der Kunde gegenüber dem Diensteanbieter ein *Wahlrecht* hinsichtlich des Speicherungsumfangs und der Speicherungsdauer von *Verbindungsdaten,* für die er entgeltpflichtig ist. Er kann dabei zwischen einer Speicherung der Verbindungsdatensätze sowohl mit vollständigen Zielnummern als auch mit um die letzten drei Ziffern verkürzten Zielnummern bis maximal 80 Tage nach Versendung der Rechnung oder der Löschung dieser Daten bei den Diensteanbietern unmittelbar nach Versendung der Rechnung wählen.

Die Liberalisierung des Telekommunikationsmarktes in Deutschland hat dazu geführt, dass Verbindungsdaten nicht mehr nur beim rechnungstellenden Diensteanbieter, sondern auch bei allen anderen Anbietern von Telekommunikationsdienstleistungen gespeichert werden, die mit dem rechnungstellenden Anbieter entweder über *Zusammenschaltungsvereinbarungen* oder die Abrechnung von *Call-by-Call-Verbindungen* vertragliche Beziehungen haben. Dies führt in der Praxis dazu, dass Verbindungsdaten in erheblichem Umfang auch bei diesen anderen Diensteanbietern gespeichert werden. Diese anderen Diensteanbieter sind bisher ebenfalls verpflichtet, die vom Kunden getroffene Wahl in der oben beschriebenen Form umzusetzen.

Nach der jetzt vorliegenden Entwurfsfassung kann der Kunde sein Wahlrecht nur noch gegenüber dem rechnungstellenden Diensteanbieter ausüben. Soweit ein Diensteanbieter nicht selbst Rechnungen stellt, wird er damit von der Löschungsverpflichtung freigestellt. Dies hätte zur Folge, dass die *Verbindungsdaten* bei allen übrigen Diensteanbietern, unabhängig von der Entscheidung des Kunden, bis zu einem halben Jahr nach Beendigung der Verbindung – die maximale Speicherdauer von bis jetzt 80 Tagen nach Versendung der Rechnung soll auf diesen Zeitraum verlängert werden – dort gespeichert bleiben.

Zum *Schutz des Beratungsgeheimnisses* dürfen Verbindungen zu Anschlüssen bestimmter *Beratungsstellen* nicht in *Einzelverbindungsnachweise* aufgenommen werden (§ 6 Abs. 8 TDSV). Hierzu müssen die Beratungsstellen bisher einen begründeten Antrag bei ihrem Telekommunikationsdiensteanbieter stellen. Die Liberalisierung des Telekommunikationsmarktes hat offenbar dazu geführt, dass dieses Verfahren nicht mehr praktikabel ist, da die verschiedenen Anbieter von Telekommunikationsdiensten unterschiedliche Maßstäbe für die Genehmigung entsprechender Anträge anlegen.

Der Entwurf zur Novellierung der TDSV sieht daher eine zentrale Bearbeitung der Anträge von Beratungsstellen durch die *Regulierungsbehörde für Telekommunikation und Post* (RegTP) vor. Allerdings ist das jetzt vorgeschlagene Verfahren noch weniger praktikabel als die bisherige Lösung: So ist vorgesehen, dass die Beratungsstellen gegenüber der RegTP ihre Aufgabenbestimmung „durch eine Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen

Rechts“ nachzuweisen haben. Diese Regelung dient offensichtlich der Entlastung der Regulierungsbehörde. Das Ziel der Änderung der TDSV, eine einheitliche Praxis bei der Bearbeitung von Anträgen von Beratungsstellen sicherzustellen, wird mit der nunmehr vorgesehenen Lösung nicht erreicht. Die Prüfung der Anträge sollte durch die RegTP selbst vorgenommen werden. Soweit der Verordnungsgeber das bereits oben beschriebene „holländische Modell“ einführen sollte, bei dem Telefonnummern nur mit ausdrücklicher Einwilligung des Betroffenen in Einzelverbindungsnachweise aufgenommen werden, sollte eine einfache Erklärung der Beratungsstelle gegenüber der Regulierungsbehörde genügen, um in die dort vorgesehene Liste aufgenommen zu werden.

Diese Liste soll öffentlich zum elektronischen Abruf bereitgestellt werden. Dies ist zu begrüßen. Gleichzeitig wird bestimmt, dass der Diensteanbieter den Inhalt der Liste sowie nachfolgende Korrekturen lediglich einmal jährlich abzufragen hat. Diese Frist ist unangemessen lang. Eine Verpflichtung der Diensteanbieter, lediglich einmal jährlich Änderungen in der Liste im eigenen Datenbestand nachzuvollziehen, bietet den Beratungsstellen keine Möglichkeit, zeitnah damit zu werben, dass Anrufe bei diesen Stellen nicht auf Einzelverbindungsnachweisen ausgewiesen werden. Es ist den Diensteanbietern durchaus zuzumuten, die von der Regulierungsbehörde bereitgestellte Liste in kürzeren Zeitabständen abzurufen. Der Zeitabstand zwischen den einzelnen Abrufen sollte nicht länger als einen Monat betragen.

Zukünftig sollen den Diensteanbietern zum Aufdecken sowie Unterbinden von *Leistungserschleichungen* und sonstigen *rechtswidrigen Inanspruchnahmen* von Telekommunikationsnetzen und -diensten Auswertungen auf dem Gesamtbestand aller Verbindungsdaten, die nicht älter als sechs Monate sind, gestattet werden. Demgegenüber sieht die TDSV bisher vor, dass täglich die Daten aus dem „Gesamtbestand aller Abrechnungszeiträume eines Monats“ verwendet werden dürfen. Als Begründung wird die Harmonisierung mit dem oben erwähnten Höchstspeicherungszeitraum für Verbindungsdaten bei Diensteanbietern genannt. Dieses Argument vermag nicht zu überzeugen. Auch ist nicht erkennbar, weshalb der Gesamtdatenbestand an Verbindungsdaten nicht – wie es noch der Vorentwurf vorsah – in anonymisierter oder zumindest pseudonymisierter Form analysiert werden kann, um dann – bei Vorliegen tatsächlicher Anhaltspunkte für Missbrauch im Einzelfall – die erforderlichen Daten personenbezogen zu speichern und auszuwerten.

Im Gegensatz zu der bisher gültigen Regelung wird durch die geplanten Bestimmungen das Angebot der fallweisen und ständigen *Rufnummernunterdrückung* für den Anrufer durch den Diensteanbieter unter den Vorbehalt des technisch Möglichen gestellt. Dies ist nicht akzeptabel. Der Vorbehalt des technisch Möglichen kann allenfalls übergangs-

weise für die neu aufgenommenen Regelungen zur Unterdrückung der Rufnummernanzeige beim Angerufenen und die „Block-Blocking"-Möglichkeit zum Abweisen „anonymer" Anrufer gelten.

Während bisher dem Anrufer eine *Anrufweiterschaltung* signalisiert werden muss, soll diese Signalisierungspflicht zukünftig entfallen. Dies ist zwar in den Fällen unbedenklich, in denen der Anrufende auf einen anderen Anschluss desselben Anschlussinhabers umgeleitet wird; der mit dem generellen Wegfall dieser Verpflichtung verbundene Verlust an Transparenz für die Anrufer ist jedoch nicht hinnehmbar.

Die Pflicht zur Kennzeichnung von Einträgen solcher Kunden in öffentlichen Verzeichnissen, die einer Aufnahme Ihrer Daten in *elektronische Verzeichnisse* widersprochen haben, soll ebenfalls ersatzlos gestrichen werden. Anders ist jedoch der Schutz solcher Personen vor dem Einlesen von Kundenverzeichnissen durch andere als den Urheber nicht zu realisieren. Dabei ist zu berücksichtigen, dass der Entwurf des Bundesinnenministeriums für ein novelliertes BDSG in § 29 Abs. 3 vorsieht, dass die Aufnahme personenbezogener Daten in elektronische oder gedruckte Verzeichnisse zu unterbleiben hat, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden (auch gedruckten) Verzeichnis ersichtlich ist. Der Datenempfänger soll außerdem sicherstellen, dass entsprechende Kennzeichnungen übernommen werden. Würde jetzt die Kennzeichnungspflicht aus der TDSV gestrichen, so liefe diese Regelung leer. Denjenigen Kunden, die nicht in elektronische Verzeichnisse aufgenommen werden wollen, bliebe weiterhin nur der Weg, ihren Eintrag aus allen – gedruckten wie elektronischen – Verzeichnissen streichen zu lassen. Dies würde aller Voraussicht nach auch dazu führen, dass der Anteil der nicht eingetragenen Teilnehmer in gedruckten Verzeichnissen zunehmen wird. Dies kann weder im Interesse der Kunden noch der Anbieter von Kundenverzeichnissen sein. Die Verpflichtung zur Kennzeichnung der Einträge sollte daher bestehen bleiben.

Auch die Vorschriften zur *Rufnummernauskunft* sollen geändert werden: So ist vorgesehen, das Verbot, Auskunft über Namen und andere Daten von Kunden zu erteilen, von denen nur die Rufnummer bekannt ist (so genannte „Invers-Auskunft"), ersatzlos entfallen zu lassen. Die Einführung einer *„Invers-Auskunft"* wäre allenfalls dann hinnehmbar, wenn sie an die ausdrückliche Einwilligung der betroffenen Anschlussinhaber gebunden würde. Die Erfahrungen bei der Einführung der „Komfort-Auskunft" im Jahr 1997 haben gezeigt, dass eine solche nachträgliche Veränderung des Nutzungszweckes von einem erheblichen Anteil der Betroffenen – zu Recht – nicht akzeptiert wird. Die Freigabe der „Invers-Auskunft" gefährdet darüber hinaus ebenfalls den Fortbestand des Auskunftsdienstes, da zu erwarten ist, dass eine erhebliche Anzahl von Nutzern die Auskunftserteilung zu ihren Daten im Hinblick darauf völlig unterbinden wird. Auch dies kann weder im Interesse der Nutzer noch der Anbieter solcher Dienste liegen.

Überwachung des Telekommunikationsverkehrs

Bereits in unserem Jahresbericht 1998 hatten wir über den Entwurf des Bundeswirtschaftsministeriums für eine *Telekommunikations-Überwachungsverordnung* (TKÜV) berichtet, die die veraltete *Fernmeldeüberwachungsverordnung* (FÜV) ersetzen sollte und nach breiter öffentlicher Kritik vom Bundeswirtschaftsministerium zurückgezogen worden war[165]. Das Bundeswirtschaftsministerium hat nunmehr im April 1999 „Eckpunkte für den Regelungsrahmen der Rechtsverordnung nach § 88 TKG“ vorgelegt.

Darin wird der – im Prinzip lobenswerte – Versuch unternommen, den Kreis der Verpflichteten, die permanente technische Vorkehrung zur Übermittlung der zu überwachenden Telekommunikation an die berechtigten Stellen vorhalten sollen, auf Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienstleistungen für die Öffentlichkeit erbracht werden, zu beschränken. Dagegen sollen Betreiber nicht-öffentlicher Netze im gewerblichen Bereich (z. B. Corporate Networks, konzerninterne Netze u. Ä.) sowie Erbringer von Telekommunikationsdiensten ohne Gewinnerzielungsabsicht (z. B. Nebenstellenanlagen, die nicht ausschließlich selbst genutzt werden, wie in Hotels, Krankenhäusern, Wohnheimen) „aus Gründen der Verhältnismäßigkeit“ nicht mehr zur Vorhaltung permanenter technischer Vorkehrungen, sondern zum „Herausfiltern“ der zu überwachenden Telekommunikation mittels externer, im Einzelfall vom Betreiber bereitzustellender Einrichtungen verpflichtet werden und dazu, die Aufzeichnung der Telekommunikation durch die berechtigte Stelle am Ort der Telekommunikationsanlage zu ermöglichen oder, falls dies technisch möglich ist, zur Weiterleitung der Telekommunikation durch die berechtigte Stelle.

Diese Tendenz zur Beschränkung des Kreises der zur permanenten Vorhaltung technischer Einrichtungen Verpflichteten ist zwar generell zu begrüßen; insgesamt wirft jedoch das Eckpunkte-Papier mehr Fragen auf als es beantwortet. So ist unklar, wie die Verpflichtungen der anderen Betreibergruppen genau aussehen sollen. Gleichzeitig macht das Eckpunkte-Papier deutlich, dass eine umfangreiche Einbeziehung der Anbieter „individueller, über das Internet abgewickelter Telekommunikationsvorgänge Gegenstand einer Überwachungsmaßnahme sein kann und dass derjenige, der entsprechende Netzzugänge anbietet, den diesbezüglichen gesetzlichen Verpflichtungen unterliegt“. Lediglich Informationsanbieter und Anbieter von Chat-Plattformen, die keine Individualkommunikation anbieten, werden ausdrücklich ausgenommen.

---

165 JB 1998, 5.2

Insgesamt zeigt sich, dass das Problem der überschießenden gesetzlichen Überwachungsbefugnisse wohl mit Hilfe von Ausnahmeregelungen auf der Verordnungsebene nicht befriedigend gelöst werden kann. Dies dürfte wohl nur im Rahmen einer entsprechenden Novellierung des Telekommunikationsgesetzes und der Revision der durch das Begleitgesetz zum Telekommunikationsgesetz erheblich erweiterten Eingriffsbefugnisse möglich sein[166].

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Bereits in den zurückliegenden Jahren hatten wir wiederholt die Ersetzung des § 12 *Fernmeldeanlagengesetz* (FAG), der eine nahezu unbeschränkte Übermittlung von Verbindungsdaten für Zwecke der *Strafverfolgung* an die entsprechenden Behörden gestattet, durch eine verfassungskonforme Regelung im Rahmen der Strafprozessordnung angemahnt[167]. Die Regelung war zuletzt im Rahmen des Begleitgesetzes zum Telekommunikationsgesetz befristet bis zum 31. Dezember 1999 verlängert worden. Der Innenausschuss des Bundestages hatte die damalige Bundesregierung aufgefordert, bis spätestens April 1998 eine verfassungskonforme Lösung im Rahmen der Strafprozessordnung zu finden, und eine Verlängerung der Geltung des § 12 FAG über das Jahr 2000 hinaus explizit abgelehnt[168].

Demgegenüber hat sich die Justizministerkonferenz auf ihrer Tagung vom 7. bis 9. Juni 1999 für eine weitere Fortgeltung des § 12 FAG auch über den 31. Dezember 1999 hinaus ausgesprochen. Ende Juni 1999 brachte die CDU/CSU-Bundestagsfraktion einen Gesetzentwurf in den Bundestag ein, der vorsah, die Befristung der Regelung einfach aufzuheben[169]. Dies hätte zur unbefristeten Fortgeltung dieser verfassungsrechtlich bedenklichen Vorschrift geführt. Beinahe zeitgleich schlug der Bundesrat an ungewöhnlicher Stelle – nämlich in seiner Stellungnahme zum Entwurf eines Gesetzes zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs – ebenfalls vor, die Befristung des § 12 FAG einfach aufzuheben[170].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Aktivitäten zum Anlass genommen, sich abermals entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG zu wenden und stattdessen eine Neufassung der Eingriffsbefugnisse unter

166 Wir hatten bereits in unserem Jahresbericht 1998 eine entsprechende Novellierung des TKG empfohlen; vgl. JB 1998, 5.2; vgl. auch das vom Berliner Datenschutzbeauftragten, dem LDA Brandenburg, dem LfD Bremen, der LfD Nordrhein-Westfalen und dem LfD Schleswig-Holstein verfasste Hintergrundpapier für eine Sicherung der freien Telekommunikation in unserer Gesellschaft unter II.1.4; Anlagenband „Dokumente zum Datenschutz 1999“, Teil B

167 vgl. zuletzt JB 1998, 5.2

168 JB 1997, 4.7.1

169 BT-Drs. 14/1315

170 BR-Drs. 325/99 unter Punkt 8; vgl. auch 4.3.1

Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz (GG) geschützten Telekommunikationsgeheimnis ergeben, zu fordern. Die Konferenz hat auch darauf hingewiesen, dass die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten sachlich in die Strafprozessordnung gehört und die gesetzlichen Zugriffsvoraussetzungen in Abstimmung mit § 100 a StPO neu geregelt werden müssen[171].

Dessen ungeachtet hat der Bundestag schließlich eine abermalige Verlängerung der Geltungsdauer des § 12 FAG für weitere 2 Jahre beschlossen[172]. Dabei wurde die Vorschrift des § 12 FAG dahingehend ergänzt, dass die Betroffenen künftig – anders als bisher – im Nachhinein von den Maßnahmen unterrichtet werden sollen. Weiterhin ist jetzt vorgeschrieben, dass die Daten vernichtet werden, wenn sie zur Strafverfolgung nicht mehr erforderlich sind. Auch eine solche Vorschrift war in der Vergangenheit im § 12 FAG nicht enthalten. Gleichzeitig haben die Koalitionsfraktionen ihren Willen bekundet, in diesem Zeitraum eine Gesamtreform der Telefonüberwachung vorzunehmen und bereits in der Übergangszeit den Datenschutz auszubauen.

Neues von ENFOPOL

Bereits im Jahresbericht 1998 hatten wir über den Entwurf für eine Entschließung des Rates der *Europäischen Union* über die rechtmäßige *Überwachung des Telekommunikationsverkehrs* in Bezug auf neue Technologien berichtet[173]. Dort war unter Bezugnahme auf die Entschließung des Rates vom 17. Januar 1995 über rechtmäßige Überwachungstelekommunikation[174] eine „Fortschreibung" der dort festgelegten Anforderungen im Hinblick auf neue Technologien, wie beispielsweise mobile satellitengestützte Dienste und öffentliche auf IT basierende (Internet-)Dienste, geplant. Nachdem eine Entwurfsfassung des Dokuments mehr oder weniger zufällig öffentlich bekannt geworden war, wurde das Vorhaben in der Presse breit kritisiert.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich zu dem Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation geäußert: In einer Entschließung vom 25./26. März 1999 betont die Konferenz, dass sie es für inakzeptabel hält, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wurde. In der Entschließung wird die Bundesregierung darüber hinaus aufgefordert, der Schaffung gemeinsamer Standards zur grenzüberschreitenden

171 Entschließung zu „ Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation", Anlagenband „Dokumente zum Datenschutz 1999", Teil A III

172 vgl. Art. 4 Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20. 12. 1999; BGBl. I S. 2491 (2492)

173 JB 1998, 5.2

174 vgl. ABlEG C 329, S. 1

Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht ein zusätzlicher Eingriff in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden ist und die Nutzung datenschutzfreundlicher Technologien (z. B. Prepaid Cards) nicht konterkariert wird[175].

Aufgrund der breiten öffentlichen Kritik ist die Entschließung unter deutscher Ratspräsidentschaft nicht mehr verabschiedet worden. Die weiteren Beratungen waren offensichtlich auch bis zum Ende des Berichtszeitraumes nicht abgeschlossen.

Über die Rechtsqualität der existierenden und der geplanten Entschließung bestehen offensichtlich sogar innerhalb der Bundesregierung Unklarheiten: In einer Antwort auf eine Große Anfrage der CDU/CSU-Fraktion hat die Bundesregierung Ende Oktober 1999 darauf hingewiesen, dass schon die oben erwähnte Ratsentschließung von 1995 mit dem Charakter einer Empfehlung an die EU-Mitgliedstaaten gefasst worden ist und ausdrücklich unter dem Vorbehalt des geltenden nationalen Rechts stehe[176]. Demgegenüber wird im „Eckpunktepapier" zur TKÜV die Ratsentschließung von 1995 unter den „. . . international abgestimmte Anforderungen an die Umsetzung von Überwachungsmaßnahmen, denen sich auch Deutschland angeschlossen hat . . .", aufgezählt[177].

Aktivitäten der G 8-Staaten zur Bekämpfung von „Hightech-Crime"

Auch die *G 8-Staaten* haben Aktivitäten zur grenzüberschreitenden Verbrechensbekämpfung im Hinblick auf das Internet und die Nutzung von Telekommunikationsdiensten entfaltet. Hierzu ist bereits im Jahr 1997 eine spezielle G 8-Arbeitsgruppe zur *„Hightech-Kriminalität"* gegründet worden. Ziel der Bemühungen ist unter anderem, die Bedingungen für die grenzüberschreitende Bekämpfung von Computerkriminalität im weitesten Sinne – hierzu werden vor allem auch Verbrechen gezählt, die unter Nutzung des Internet begangen werden – zu erreichen.

Neben einer generellen Verpflichtung aller Anbieter von Internet-Dienstleistungen, Verbindungsdaten über die Aktivitäten ihrer Kunden generell für einen bestimmten Zeitraum zur Nutzung für eine eventuelle, spätere Strafverfolgung zu speichern, werden in der Arbeitsgruppe auch Modelle diskutiert, die mit geringeren Eingriffen in das informationelle Selbstbestimmungsrecht der Nutzer von Internet-Diensten verbunden sind: So wurde vorgeschlagen, die Anbieter von Internet-

175 Entschließung zu „Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)", Anlagenband „Dokumente zum Datenschutz 1999", Teil A I;
176 vgl. BT-Drs. 14/1866, S. 12, Punkt 14
177 vgl. DuD 12/99, S. 719, Fn. 13

Dienstleistungen dazu zu verpflichten, auf Antrag einer Strafverfolgungsbehörde aus einem Drittland Verbindungsdaten eines bestimmten Nutzers für einen gewissen Zeitraum „einzufrieren", bis festgestellt werden kann, ob die Weitergabe dieser Daten an die ausländische Strafverfolgungsbehörde unter den Bedingungen des für den Internet-Anbieter geltenden nationalen Rechts zulässig ist (*„Fast freeze – quick thaw"*). Offen ist allerdings, inwieweit ein solches Vorgehen mit dem bisher geltenden deutschen Recht vereinbar wäre.

Auf der Konferenz der Justiz- und Innenminister der G 8-Staaten in Moskau am 19. und 20. Oktober 1999 wurde eine Einigung dahingehend erzielt, dass unter Berücksichtigung der Grundsätze in Bezug auf die Souveränität der Einzelstaaten und den Schutz der Menschenrechte, der demokratischen Freiheiten und der Privatsphäre Strafverfolgungsbehörden bei der Durchführung strafrechtlicher Ermittlungen unter bestimmten Umständen über territoriale Grenzen hinweg ermitteln können sollen. Hinsichtlich des Zugriffs auf im Ausland gespeicherte Daten haben sich die Minister auf einen Katalog von Grundsätzen geeinigt[178]. Unter anderem soll jeder Staat sicherstellen, dass er in der Lage ist, für eine schnelle Sicherung von Daten zu sorgen, die in einem Computersystem gespeichert sind, insbesondere von Daten, die im Besitz von Dritten, z. B. Diensteanbietern, sind und die in der Regel nur kurzfristig zurückbehalten werden oder bei denen anderweitig Verlust oder Veränderung droht, damit der Zugriff darauf, ihre Feststellung, Vervielfältigung, Erhebung oder Herausgabe beantragt werden kann. Es soll dafür gesorgt werden, dass eine Sicherung auch dann möglich ist, wenn sie nur erforderlich ist, um einem anderen Staat Rechtshilfe zu leisten. Die Teilnehmerstaaten haben sich verpflichtet, durch internationale Zusammenarbeit, Übereinkünfte und innerstaatliche Gesetze auf die Durchführung dieser Grundsätze hinzuwirken.

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten („Art. 29-Gruppe") hat in ihrer Empfehlung zur Speicherung von Verbindungsdaten durch Internet-Service-Provider für Zwecke der Strafverfolgung vom 7. September 1999 eine prinzipielle Verpflichtung der Internet-Service-Provider, Verbindungsdaten ausschließlich für Zwecke der Strafverfolgung zu speichern, abgelehnt. Die Betreiber von Telekommunikationsnetzen und -diensten sowie Internet-Service-Provider sollen nicht verpflichtet werden, Verbindungsdaten über den für die Abrechnung von Dienstleistungen erforderlichen Zeitraum hinaus zu speichern. Die Arbeitsgruppe hat darüber hinaus der Europäischen Kommission empfohlen, geeignete Maßnahmen zu treffen, um die Speicherungsdauer für Verbindungsdaten bei Betreibern von Telekommunikationsnetzen und -diensten sowie Internet-Service-

178 Ministerkonferenz der G 8-Staaten zur Bekämpfung transnationaler organisierter Kriminalität, Moskau 19./20. 10. 1999: Ministererklärung zur Hightech-Kriminalität, Anlage 1

Providern für die Abrechnung von Dienstleistungen untereinander und mit ihren Kunden weiter zu harmonisieren[179].

5.2 Tele- und Mediendienste

Die Internet-Begeisterung in der deutschen Bevölkerung scheint ungebrochen, wenngleich die Nutzung der neuen elektronischen Dienste im Bereich des elektronischen Handels offensichtlich bisher hinter den Erwartungen der Anbieter solcher Dienste zurückbleibt. Dies ist offensichtlich nicht zuletzt der Befürchtung eines großen Prozentsatzes der Nutzer geschuldet, dass ihre personenbezogenen Daten im Internet missbraucht werden könnten: Einer Meldung des Handelsblatts vom Oktober 1999 zufolge besitzen zwar 6,67 Millionen Bundesbürger (10,5 % der Bevölkerung ab 14 Jahren) privat einen Computer mit Online-Zugang[180]. Nach Angaben des Blattes erledigen jedoch nur 35 % von ihnen z. B. ihre Geldgeschäfte per Online-Banking. Als Hauptgrund für die Zurückhaltung nennen 51 % der potenziellen Nutzer die Furcht vor unzureichendem Datenschutz.

Insgesamt war im zurückliegenden Berichtszeitraum wiederum ein Anstieg der Beratungsersuchen von Bürgern im Bereich der Tele- und Mediendienste zu verzeichnen. Gleichzeitig haben sich auch zahlreiche Anbieter solcher Dienste mit Beratungsersuchen an uns gewandt. Dies deutet darauf hin, dass bei einem erheblichen Anteil der Anbieter von *Tele- und Mediendiensten* nach wie vor Unklarheit über das anzuwendende Recht und die sich aus dem geltenden Recht ergebenden Konsequenzen hinsichtlich der Gestaltung von Internet-Angeboten besteht.

Evaluierung des Informations- und Kommunikationsdienstegesetzes (IuKDG)

Im zurückliegenden Berichtszeitraum hat die Bundesregierung ihren Bericht über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienstegesetzes *(IuKDG)* vorgelegt[181]. Wir haben im Auftrag der Konferenz der Obersten Aufsichtsbehörden für den Datenschutz im privaten Bereich (des sog. „Düsseldorfer Kreises“) zur *Evaluierung* des IuKDG eine umfangreiche Stellungnahme abgegeben; zahlreiche der dort angesprochenen Punkte sind von der Bundesregierung in ihrem Bericht berücksichtigt worden[182].

---

179 Recommendation 3/99 on the Preservation of Traffic Data by Internet Service Providers for Law Enforcement Purposes; Dok. 5085/99/EN/Final WP 25

180 vgl. Handelsblatt v. 21. 10. 1999, S. 33

181 vgl. BT-Drs. 14/1191

182 Die wesentlichen Inhalte unserer Anregungen haben wir bereits im Jahresbericht 1998 veröffentlicht, vgl. ebenda 5.3

Nach dem gegenwärtigen Entwurfsstand zur Novellierung des Bundesdatenschutzgesetzes plant die Bundesregierung, einige der zentralen Elemente aus dem Teledienstedatenschutzgesetz (TDDSG, Art. 2 des IuKDG) in das BDSG zu übernehmen. Dazu zählen unter anderem die Verpflichtung der Anbieter zur datensparsamen Gestaltung ihrer Dienste (§ 3 Abs. 4 TDDSG), die Verpflichtung der Anbieter, die Nutzung von Diensten anonym oder unter Pseudonym zu ermöglichen (§ 4 Abs. 1 TDDSG), und die Einführung eines „Datenschutz-Audits", wie es jetzt bereits im Mediendienste-Staatsvertrag vorgesehen ist (§ 17 MDStV). Soweit es sich dabei um Vorschriften aus dem TDDSG handelt, sollen diese nach der Novellierung des BDSG aus dem TDDSG gestrichen werden.

Übermittlung von Bestandsdaten von Nutzern von Telediensten an das Bundesamt für Verfassungsschutz

Das Bundesamt für Verfassungsschutz hatte an einen Berliner Internet-Service-Provider eine Anfrage gerichtet, in der um Mitteilung von Bestandsdaten zu einer E-Mail-Adresse unter Berufung auf § 3 Abs. 1 Bundesverfassungsschutzgesetz gebeten wurde. Der Service Provider wandte sich an uns mit der Bitte um datenschutzrechtliche Überprüfung.

Beim Angebot von E-Mail-Diensten handelt es sich um einen *Teledienst* im Sinne des Teledienstedatenschutzgesetzes (TDDSG). Die Befugnisse und Verpflichtungen zur Verarbeitung personenbezogener Daten bei den Anbietern solcher Dienstleistungen richten sich mithin nach den Vorschriften dieses Gesetzes. Bei dem vom Bundesamt für Verfassungsschutz angeforderten Inhaberdaten handelt es sich um Bestandsdaten im Sinne des § 5 TDDSG.

Im Gegensatz zu dem für Anbieter von Telekommunikationsdiensten gültigen Telekommunikationsgesetz (vgl. §§ 88, 89 Abs. 6, 90 TKG) enthalten das Teledienstegesetz sowie das Teledienstedatenschutzgesetz keine Verpflichtung bzw. Berechtigung für Anbieter von Telediensten, Sicherheitsbehörden die Bestandsdaten ihrer Kunden zu übermitteln. Die Anbieter solcher Dienstleistungen sind daher weder verpflichtet noch berechtigt, solchen Anliegen des Bundesamtes für Verfassungsschutz oder anderer Nachrichtendienste zu entsprechen.

Nutzung personenbezogener Kundendaten

Uns haben mehrere Eingaben erreicht, die sich mit der Ausgestaltung der *Allgemeinen Geschäftsbedingungen* (AGB) von *Internet-Diensteanbietern* befassten. Festzustellen ist, dass hinsichtlich der datenschutzgerechten Ausgestaltung von Allgemeinen Geschäftsbedingungen offensichtlich bei zahlreichen Anbietern nach wie vor Unklarheiten bestehen.

Ein Petent hatte sich bei einem Berliner Internet-Diensteanbieter eine Internet-Domain reservieren lassen. Bei Vertragsschluss wurde auf die AGB des Unternehmens hingewiesen, in denen unter anderem bestimmt wird, dass das Unternehmen personenbezogene Daten des Kunden für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste nutzen und verarbeiten darf. Die Bestandsdaten sind solche Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telediensten erforderlich sind. Der Kunde sei jedoch nicht verpflichtet, dieser Regelung zuzustimmen.

Bei dem Angebot handelt es sich um einen *Teledienst* nach § 2 Abs. 2 Nr. 5 Teledienstgesetz. Nach § 5 Abs. 2 TDDSG ist eine Verarbeitung und Nutzung von *Bestandsdaten* für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste nur zulässig, soweit der Nutzer in diese ausdrücklich eingewilligt hat. Die oben zitierte Bestimmung der AGB des Internet-Dienstleisters ist dagegen faktisch als Widerspruchslösung ausgestaltet, die keine ausdrückliche Einwilligung vorsieht, sondern dem Kunden anheim stellt, eine bereits vorhandene Regelung zu streichen. Der betreffende Teil der AGB des Anbieters war in der vorliegenden Form auch deswegen rechtswidrig, weil generell die Herbeiführung von Einverständniserklärungen durch AGB nach höchstrichterlicher Rechtsprechung unzulässig ist[183].

Unterrichtungspflichten des Anbieters

§ 3 Abs. 5 TDDSG sieht vor, dass der Nutzer vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten ist. Der Inhalt der Unterrichtung muss für die Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren.

Ein Petent hatte bei einem Berliner Internet-Service-Provider die Einrichtung einer .de-Domain beantragt. Hierzu hat das Unternehmen – datenschutzrechtlich völlig korrekt – die notwendigen Bestandsdaten bei dem Kunden erhoben. Dieser war davon ausgegangen, dass seine Daten durch das Unternehmen nicht an Dritte weitergegeben würden. Umso erstaunter war er, als er feststellen musste, dass sein Name, seine Adresse und seine Telefonnummer in einer im Internet öffentlich zugänglichen Datenbank veröffentlicht wurden. Hierauf hatte das Unternehmen den Kunden im Rahmen seiner AGB hingewiesen.

183 vgl. BGH, Urteil v. 16. 3. 1999, Az.: XI ZR 76/98 und BGH, Urteil v. 24. 3. 1999, Az.: IV ZR 90/98

Tatsächlich wird die Registrierung von so genannten „Second-Level-Domains“ in der „Country Code Top Level *Domain“* „.de“ (dazu zählen z. B. Internet-Adressen wie die von unserer Behörde verwendete Adresse „datenschutz-berlin.de“) nicht durch die verschiedenen Anbieter von Internet-Dienstleistungen, sondern zentral durch die in Frankfurt am Main ansässige *DENIC e. G.* Deutschland-weit vorgenommen. Unternehmen wie das oben genannte Berliner Unternehmen bieten diese Dienstleistung nicht selbst an, sondern vermitteln sie lediglich. Die Allgemeinen Geschäftsbedingungen der DENIC e. G. sehen vor, dass für jeden Domain-Inhaber dessen Namen, Adresse und Telefonnummer in der *„Whols-Datenbank“* der DENIC im Internet veröffentlicht werden.

Auch die AGB des Berliner Anbieters enthielten einen Hinweis darauf, dass die entsprechenden Daten an die DENIC übermittelt und dort im Internet veröffentlicht würden. Der Diensteanbieter ist damit seiner *Unterrichtungspflicht* nach § 3 Abs. 5 TDDSG nicht in hinreichender Weise nachgekommen. In den von dem Anbieter verwendeten Online- und Offline-Formularen wurde lediglich in allgemeiner Form auf die AGB hingewiesen; ein Hinweis auf die beabsichtigte Verarbeitung der erhobenen personenbezogenen Daten – wie in § 3 Abs. 5 TDDSG vorgeschrieben – erfolgte jedoch nicht. Dies widerspricht den gesetzlichen Bestimmungen für die Erfüllung der Informationspflichten des Anbieters. Gemäß § 3 Abs. 5 TDDSG reicht ein einfacher Hinweis (z. B. ein Link) auf die AGB des Anbieters nicht aus. Gleiches gilt auch für das Angebot von Mediendiensten: Die in § 12 Abs. 6 MDStV vorgesehene Unterrichtungspflicht für Anbieter von Mediendiensten entspricht den Regelungen des TDDSG.

Verarbeitung von Nutzungsdaten im Arbeitsverhältnis in der öffentlichen Verwaltung

Bereits in unserem Jahresbericht 1998 hatten wir umfangreich über Fragen der Geltung des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrages (MDStV) im *Arbeitsverhältnis* berichtet[184] und darauf hingewiesen, dass die Vorschriften von TDDSG und MDStV nicht anzuwenden sind, soweit die entsprechenden Dienste den Arbeitnehmern ausschließlich zur dienstlichen Nutzung zur Verfügung gestellt werden. Eine *Protokollierung der dienstlichen Nutzung von Telediensten* ist im Rahmen der arbeitsrechtlichen Erfordernisse („Offline-Recht“) gestattet. Diese Erfordernisse müssen in jedem Einzelfall geprüft werden. Eine Vollprotokollierung aller Einzelzugriffe eines Arbeitnehmers im Word Wide Web ist jedoch unverhältnismäßig. Gleichzeitig muss bei der Auswertung von Nutzungsdateien über die

184 JB 1998, 5.3

dienstliche Nutzung von Diensten darüber hinaus § 31 Bundesdatenschutzgesetz (BDSG) beachtet werden, der für solche Daten eine besondere *Zweckbindung* vorsieht.

Der Berliner Senat hat darauf hingewiesen, dass durch Arbeitsanweisung zur Nutzung von Online-Diensten in den Behörden eine Regelung gegeben ist, die den dienstlichen Charakter der Nutzung der Anwendung hervorhebt. Die private Nutzung ist darin ausgeschlossen, kann aber technisch nicht verhindert werden. Durch stichprobenartige Auswertung der Log-Protokolle ist nach Auffassung des Senats die Einhaltung der Regeln zu kontrollieren[185]. Offensichtlich geht der Senat davon aus, dass *Log-Protokolle* über die dienstliche Nutzung in jedem Fall bei den öffentlichen Stellen des Landes Berlin geführt werden bzw. geführt werden müssen.

Diese Auffassung verkennt jedoch, dass die Protokollierung der Nutzung von Tele- und Mediendiensten – soweit sie nicht aus Datensicherheitsgründen geboten ist – im Regelfall nicht als erforderlich im Sinne des § 28 BDSG angesehen werden kann. Eine Protokollierung des Nutzerverhaltens einzelner Arbeitnehmer kann lediglich im Einzelfall zulässig sein, soweit tatsächliche Anhaltspunkte für entsprechende arbeitsvertragliche Verstöße vorliegen. Dagegen ist die vorauseilende Vollprotokollierung und deren stichprobenartige Auswertung im Regelfall unzulässig.

5.3 Datenschutz und Medien

Rundfunk-Abgabe statt Gebühr – ein datenschutzfreundlicher Vorschlag

Im November 1999 wurde in der Presse berichtet, dass es in der CDU konkrete Überlegungen gäbe, die gerätebezogene *Rundfunk- und Fernsehgebühr* abzuschaffen und stattdessen eine allgemeine Abgabe pro Einwohner für die Grundversorgung mit Informationen einzuführen[186]. Das Modell zielt auf eine Abschaffung der *Gebühreneinzugszentrale* (GEZ) und die Erhebung einer Abgabe von allen erwachsenen Bürgern, unabhängig davon, ob sie ein Runkfunk- oder ein Fernsehgerät besitzen oder nicht. Nach den in der Presse zitierten Angaben des Vorsitzenden des Bundesfachausschusses Medien der CDU könne die neue Abgabe höchstens die Hälfte der derzeitigen GEZ-Gebühr betragen, da mit diesem System die Verwaltungskosten für die GEZ entfielen, die Kosten auf alle Einwohner verteilt und auch diejenigen Bürger erfasst würden, die bisher keine Rundfunkgebühr zahlen, obwohl sie Rundfunkgeräte zum Empfang bereithalten.

185 vgl. Abghs.-Drs. 13/3817, S. 153
186 vgl. Berliner Morgenpost v. 14. 11. 1999, S. 18

Dieser Vorschlag ist aus Datenschutzsicht sehr zu begrüßen: Bereits in der Vergangenheit hatten wir mehrfach darauf hingewiesen, dass die von der GEZ bereitgehaltenen Datenbestände der Rundfunkteilnehmer aufgrund des großen Anteils der Rundfunkteilnehmer an der Gesamtbevölkerung praktisch einem *„Bundesmelderegister"* gleichkommen, das in der Rechtsordnung der Bundesrepublik Deutschland aus guten Gründen nicht vorgesehen ist. Diese Datenbestände wecken immer wieder auch Begehrlichkeiten Dritter, die sie für ihre Zwecke (z. B. zur Beitreibung öffentlich-rechtlicher Forderungen)[187] nutzen wollen.

Auch hat der Versuch der Rundfunkanstalten, Personen aufzufinden, die bisher keine Rundfunkgebühr zahlen, obwohl sie Geräte zum Empfang bereithalten, in der Vergangenheit zu datenschutzrechtlich bedenklichen Entwicklungen geführt: So wurde mit dem Argument der Schaffung von Gebührengerechtigkeit im Jahre 1997 auch im Land Berlin – trotz unserer ablehnenden Stellungnahme[188] – die regelmäßige Übermittlung von Meldedaten durch das Landeseinwohneramt an den Sender Freies Berlin eingeführt.

Auch die Tätigkeit der *„Rundfunkgebührenbeauftragten",* die im Auftrag des *SFB* säumige Rundfunkteilnehmer auffinden sollen, führte und führt immer wieder zu Irritationen in der Bevölkerung. Gleiches gilt auch für die Maßnahmen der GEZ, die durch die massenweise Versendung von so genannten „werblichen Schreiben" ebenfalls versucht, den Prozentsatz zahlender Rundfunkteilnehmer anzuheben.

All diese Aktivitäten, die jeweils mit teilweise erheblichen Eingriffen in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sind, könnten bei der Ersetzung der teilnehmerbezogenen Rundfunkgebühr durch eine entsprechende Abgabe entfallen: Die riesigen Datenbestände bei der GEZ wären entbehrlich, ebenso die zweckfremde Nutzung von Daten aus den Melderegistern zum Zwecke der Beitreibung von Rundfunkgebühren. Auch die Aktivitäten der Rundfunkgebührenbeauftragten, die von vielen Bürgern als „Schnüffelei" empfunden werden, könnten ersatzlos eingestellt werden. Möglicherweise könnte auch die Erhebung, Speicherung und Nutzung teilweise sehr sensibler Daten bei Sozialämtern, dem SFB und der GEZ zum Zweck der Befreiung von der Rundfunkgebühr entfallen.

Statt der eigens zum Zwecke der Beitreibung und Verwaltung von Rundfunkgebühren aufgebauten, umfangreichen und teuren Infrastruktur bei der Gebühreneinzugszentrale könnten die sowieso vorhandenen Einrichtungen der Finanzämter zur Erhebung einer Rundfunk-Abgabe genutzt werden.

---

187 vgl. z. B. H. Hagemann: Vollstreckungs- und Ermittlungsmöglichkeiten gegen Schuldner mit unbekanntem Aufenthalt. In: Kommunal-Kassen-Zeitschrift 7/99, S. 148 ff. (150)

188 JB 1996, 4.2.1

5.3

Vierter Rundfunkänderungsstaatsvertrag

Mit dem Vierten Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (Vierter *Rundfunkänderungsstaatsvertrag*)[189] soll unter anderem die Einführung des „digitalen Fernsehens“ sowie neuer Rundfunkdienste geregelt werden. Die datenschutzrechtlichen Bestimmungen des Rundfunkstaatsvertrages sind in enger Abstimmung zwischen den Landesdatenschutzbeauftraten und den Staats- und Senatskanzleien der Länder überarbeitet worden.

Die Vorschriften entsprechen weitgehend den bereits jetzt gültigen Bestimmungen des Mediendienste-Staatsvertrages[190]; die – minimalen – Abweichungen zwischen den beiden Regelungen sind den besonderen technischen Bedingungen des Rundfunks geschuldet.

Die Einführung weitgehend gleichartiger materieller Datenschutzregelungen für die Bereiche Mediendienste und Rundfunk ist besonders unter dem Aspekt des zunehmenden Zusammenwachsens dieser beiden Bereiche zu begrüßen. Dadurch wird nicht nur ein *gleichmäßig hoher Datenschutzstandard für die Benutzer von Medien- und Rundfunkdiensten* sichergestellt, sondern gleichzeitig auch eine weitgehende Rechtssicherheit für die Anbieter von Diensten geschaffen, die sich auf der Schnittstelle zwischen Medien- und Rundfunkdiensten bewegen.

Besonders wichtig wird in der Zukunft die Entwicklung und Einführung *anonymer bzw. pseudonymer Nutzungsformen* durch die Anbieter neuer Rundfunkdienste sein, um eine Nutzerprofilbildung hinsichtlich des Mediennutzungsverhaltens zu verhindern.

Der Staatsvertrag soll durch Zustimmungsgesetz bis zum 1. April 2000 in Kraft treten. Gleichzeitig ist – wie bereits im letzten Jahresbericht angemerkt[191] – der *Rundfunk-Staatsvertrag Berlin – Brandenburg* mit der Verabschiedung des 4. Rundfunkänderungsstaatsvertrages erneut überarbeitungsbedürftig geworden. Wir gehen davon aus, dass die entsprechende Novellierung im Laufe des Jahres 2000 auf den Weg gebracht werden wird.

Umfang der Auskunftspflicht von Rundfunkteilnehmern nach § 4 Abs. 5 des Rundfunkgebührenstaatsvertrages

Im Frühjahr des Berichtszeitraumes wandten sich mehrere Berliner Rundfunkteilnehmer an uns, die von der im Auftrag des Senders Freies Berlin (SFB) tätigen Gebühreneinzugszentrale (GEZ) Post erhalten hatten. Die Petenten hatten bei der GEZ zwar Hörfunkgeräte, aber keine Fernsehgeräte angemeldet. Der SFB begehrte Auskunft darüber, ob

189 Abghs.-Drs. 13/3987
190 JB 1997, 4.7.4
191 JB 1998, 4.5

unterdessen auch Fernsehgeräte zum Empfang bereitgehalten würden. Die Petenten wandten sich an uns mit der Frage, ob diesbezüglich eine Verpflichtung zur Auskunftserteilung besteht.

Alle Berliner Rundfunkteilnehmer, die nur Hörfunk-, aber keine *Fernsehgeräte* angemeldet haben, erhielten derartige Schreiben der GEZ. Ein beiliegendes Formular kann zur Anmeldung mittlerweile ggf. vorhandener Fernsehgeräte verwandt werden; das Formular enthält ebenfalls eine Rubrik, in der dem SFB mitgeteilt wird, dass weiterhin keine Fernsehgeräte durch den Rundfunkteilnehmer zum Empfang bereitgehalten werden. Der SFB vertritt die Auffassung, dass Rundfunkteilnehmer sowohl in den Fällen zur *Auskunft* gegenüber dem SFB (d. h. zur Rücksendung des ausgefüllten Formulars) verpflichtet sind, wenn unterdessen Fernsehgeräte zum Empfang bereitgehalten werden, als auch in den Fällen, in denen weiterhin kein Fernsehgerät im Haushalt vorhanden ist. Der SFB stützt dies auf die Regelung des § 4 Abs. 5 Rundfunkgebührenstaatsvertrag, nach der „. . . die zuständige Landesrundfunkanstalt . . . vom Rundfunkteilnehmer oder von Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie ein Rundfunkgerät zum Empfang bereithalten und dies nicht oder nicht umfassend nach § 3 Abs. 1 und 2 angezeigt haben, Auskunft über diejenigen Tatsachen verlangen [kann], die Grund, Höhe und Zeitraum ihrer Gebührenpflicht betreffen." Nach Auskunft des SFB bzw. der GEZ sollen derartige Mailing-Aktionen zukünftig in jährlichen Abständen wiederholt werden.

Während für diejenigen Personen, die unterdessen ein Fernsehgerät zum Empfang bereithalten, zweifelsohne eine Anzeige- und damit auch eine Auskunftspflicht gegenüber dem SFB bzw. der GEZ besteht, ist die Auffassung des SFB unzutreffend, dass eine Auskunftspflicht auch dann bestehe, wenn weiterhin keine Fernsehgeräte zum Empfang bereitgehalten werden. Die in Rede stehende Vorschrift begründet im Gegenteil keine Verpflichtung der Rundfunkteilnehmer, auch Auskunft darüber zu erteilen, dass *kein* Fernsehgerät zum Empfang bereitgehalten wird. Die Vorschrift bestimmt lediglich, dass die Landesrundfunkanstalt Auskunft über diejenigen Tatsachen verlangen kann, die Grund, Höhe und Zeitraum der *Gebührenpflicht* der Rundfunkteilnehmer betreffen. Eine Auskunftspflicht besteht mithin nur, soweit auch eine entsprechende Gebührenpflicht besteht (also ein Fernsehgerät bereitgehalten wird). Ist dies nicht der Fall, so ist der Rundfunkteilnehmer nicht verpflichtet, dem SFB Auskunft darüber zu erteilen, dass weiterhin kein Fernsehgerät zum Empfang bereitgehalten wird. § 4 Abs. 5 des Rundfunkgebührenstaatsvertrages verpflichtet nicht zu einer derartigen *„Negativ-Auskunft"*.

Diese Rechtsauffassung wird von den anderen Landesbeauftragten für den Datenschutz, die eine eigene Kontrollkompetenz im wirtschaftlich-administrativen Bereich ihrer Landesrundfunkanstalten haben

(dies betrifft die Landesbeauftragten Bremen, Hessen und den LDA Brandenburg), geteilt.

Wir haben sowohl den Petenten als auch dem SFB unsere oben geschilderte Rechtsauffassung mitgeteilt und gehen davon aus, dass der SFB die verwendeten Formulare so umgestalten wird, dass eine Auskunftspflicht nur noch in den Fällen angeführt wird, in denen tatsächlich Fernsehgeräte zum Empfang bereitgehalten werden.

Datenschutz und Presse

Im Zuge der laufenden Novellierung des Bundesdatenschutzgesetzes (BDSG) ist unter anderem beabsichtigt, zur Umsetzung der Allgemeinen Datenschutzrichtlinie der Europäischen Union (Richtlinie 95/46/EG) den Geltungsbereich bestimmter Vorschriften des BDSG auch auf Unternehmen und Hilfsunternehmen der Presse hinsichtlich der Verarbeitung personenbezogener Daten zu eigenen journalistisch-redaktionellen, künstlerischen oder literarischen Zwecken auszudehnen (§ 41 Abs. 1 BDSG-E)[192]. Unter anderem ist vorgesehen, auch die Presseunternehmen zur *Bestellung eines internen, betrieblichen Datenschutzbeauftragten* zu verpflichten, der über die Einhaltung der Datenschutzbestimmungen im journalistisch-redaktionellen Bereich wachen soll; außerdem wird den Betroffenen von der Berichterstattung ein – wenngleich eingeschränktes – *Recht auf Auskunft* über die zu ihrer Person bei Presseunternehmen gespeicherten personenbezogenen Daten eingeräumt.

Gegen diese Überlegungen ist vonseiten der Presse und deren Verbänden – insbesondere dem *Deutschen Presserat* – scharfe Kritik erhoben worden. So hat der Deutsche Presserat im August 1999 eine umfangreiche Stellungnahme veröffentlicht, in der die vorgeschlagene Änderung des BDSG rundheraus abgelehnt wird[193]. Das daraus resultierende Presseecho reichte von sachlicher Kritik bis hin zu polemischen Übertreibungen, nach denen die geplanten Änderungen auf eine „Zensur“ und die Schaffung von „Staatsbeauftragten in den Redaktionen“ abzielten. Die Bundesregierung hat daraufhin verkündet, die Formulierungen des § 41 des Referentenentwurfs zum BDSG nochmals zu überdenken.

Selbstverständlich kann eine wie immer geartete Gefährdung der *Pressefreiheit* nicht Ziel des Datenschutzes sein. Jedoch sind die Behauptungen in der Presse, nach denen die beabsichtigte Neufassung des BDSG eben in einer solchen Gefährdung der Pressefreiheit resultieren würde, kaum nachzuvollziehen: Entsprechende Regelungen werden im Medienbereich bereits seit längerem erfolgreich praktiziert, ohne dass dies zu einer erkennbaren Einschränkung der Pressefreiheit

192 vgl. 1.1
193 http:/www.presserat.de/stellungnahme.pdf

geführt hat. So ist die in Rede stehende Verpflichtung zur Bestellung eines internen Datenschutzbeauftragten im Entwurf zum BDSG bereits jetzt für den Sender Freies Berlin (SFB) im Berliner Datenschutzgesetz enthalten (vgl. § 31 Abs. 3 BlnDSG). Auch die übrigen Landesrundfunkanstalten haben entsprechend Datenschutzbeauftragte für den journalistisch-redaktionellen Bereich bestellt. Der in der Öffentlichkeit scharf kritisierte Auskunftsanspruch über gespeicherte personenbezogene Daten besteht nach Berliner Landesrecht gegenüber dem SFB (vgl. § 31 Abs. 1 i. V. m. § 16 BlnDSG) und den übrigen privaten und öffentlich-rechtlichen Rundfunkanbietern in Berlin und Brandenburg[194] ebenfalls bereits jetzt. Vergleichbare Auskunftsregelungen existieren auch in den meisten anderen Bundesländern für den Bereich des öffentlich-rechtlichen Rundfunks[195].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits am 9./10. März 1995 in Bremen in einer Entschließung darauf hingewiesen, dass der Schutz des informationellen Selbstbestimmungsrechts im Medienbereich insgesamt – wenngleich unter umfassender Wahrung des Schutzes der Pressefreiheit – verbesserungsbedürftig ist[196].

Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation

Die Arbeitsgruppe ist im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten 1983 auf Initiative des Berliner Datenschutzbeauftragten gegründet worden, unter dessen Vorsitz sie nach wie vor arbeitet, und hat seither eine Vielzahl von Empfehlungen zur Verbesserung des Datenschutzes in der Telekommunikation erarbeitet. Teilnehmer sind Datenschutzbehörden, aber auch Regierungsstellen, Vertreter internationaler Organisationen und Wissenschaftler aus aller Welt. Seit Anfang der 90er Jahre gilt das besondere Augenmerk der Arbeitsgruppe der Wahrung der *Persönlichkeitsrechte im Internet.* In drei „Gemeinsamen Standpunkten" hat sie die Bedeutung der informationellen Selbstbestimmung bei neuen Entwicklungen bei der Telekommunikation betont:

– Alle Betroffenen müssen das Recht haben, der *Veröffentlichung von Bilddateien,* z. B. von Bildern des eigenen Wohngebäudes, insbesondere deren kommerziellen Nutzung zu widersprechen[197].

---

194 vgl. § 58 Staatsvertrag über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks v. 29. 2. 1992

195 vgl. die Übersicht im Bericht für die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. 3. 1995 in Bremen zu Medien- und Persönlichkeitsschutz; Materialien zum Datenschutz Bd. 23, Berlin 1996

196 vgl. Entschließung der 49. Konferenz am 9./10. 3. 1995 in Bremen zu Anforderungen an den Persönlichkeitsschutz im Medienbereich, JB 1995, Anlage 2.5

197 Gemeinsamer Standpunkt der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation zum Datenschutz bei Gebäude-Bilddatenbanken, Anlagenband „Dokumente zum Datenschutz 1999", Teil C; vgl. auch 4.6.4

- Alle Betroffenen müssen beim *Einsatz „intelligenter Software-Agenten",* die z. B. bei der Verwaltung von Netzwerkressourcen oder zur Suche nach bestimmten Informationen im Internet eingesetzt werden, so weit wie möglich über die Funktionsweise aufgeklärt werden[198].
- Der *Einsatz von Spracherkennungs- und -analysetechniken* ist nur auf der Grundlage der ausdrücklichen Zustimmung der Betroffenen zulässig, die Auswertung von Daten zur Bestimmung des geistigen oder psychischen Zustands der Betroffenen ist auszuschließen[199].

Die Dokumente enthalten daneben eine Vielzahl weiterer Empfehlungen, insbesondere zum Einsatz von Technologien, die möglichst sparsam mit der Verarbeitung personenbezogener Daten umgehen, in den jeweiligen Bereichen.

Weitere Themen waren Datenschutzprobleme bei der Vergabe von Domainnamen im Internet, bei der Bannerwerbung in Webangeboten und bei der Speicherung von Verkehrsdaten in Telekommunikationsnetzen.

198 Gemeinsamer Standpunkt zu intelligenten Software-Agenten, Anlagenband „Dokumente zum Datenschutz 1999", Teil C

199 Gemeinsamer Standpunkt zur Sprechererkennung und zur Sprachanalyse bei der Telekommunikation, Anlagenband „Dokumente zum Datenschutz 1999", Teil C

6. Aus der Dienststelle

6.1. 20 Jahre Datenschutz in Berlin

Die Dienststelle des *Berliner Datenschutzbeauftragten* nahm vor 20 Jahren ihre Arbeit auf. Nachdem das Berliner Datenschutzgesetz am 12. Juli 1978 verabschiedet worden war, hatte es einige Monate gedauert, bis der vormalige Direktor der Datenverarbeitungszentrale Baden-Württemberg Dr. Hans-Joachim *Kerkau* am 27. September 1979 zum ersten Berliner Datenschutzbeauftragten gewählt wurde. Mit seiner Sekretärin Monika Klößing begann er am 1. November 1979 im Europacenter, die Einhaltung der Datenschutzvorschriften durch die Berliner Verwaltung zu kontrollieren. Schon sehr bald stellte sich heraus, dass neben der Bearbeitung der vielen Beschwerden, die die Dienststelle erreichten, die Beratung der Verwaltung zur Verbesserung des Datenschutzes, vor allem aber auch die Beratung des Berliner Gesetzgebers die wichtigsten Aufgaben darstellen.

In den ersten zehn Jahren wurde der Grundstein gelegt für das Renommee, das der Berliner Datenschutzbeauftragte seither insbesondere auf dem Gebiet des Datenschutzes in der Telekommunikation genießt. Im September 1983 traf sich anlässlich der Internationalen Funkausstellung zum erstenmal die Internationale Arbeitsgruppe Datenschutz bei der Telekommunikation der Internationalen Konferenz der Datenschutzbeauftragten, die heute unter dem Namen „Berlin Group“ weltweit bekannt ist. Anlass für diesen Schwerpunkt war der Umstand, dass im Mai 1980 mit dem *Bildschirmtext-Erprobungsgesetz* in Berlin erstmals ein Gesetz geschaffen wurde, das den Datenschutz bei den „Neuen Medien“ regelt. Die dort und im Bildschirmtext-Staatsvertrag vom März 1983 enthaltenen Bestimmungen dienen seither als Vorlage für alle Regelungen zum Datenschutz in der Telekommunikation bis hin zu Teledienstedatenschutzgesetz und Mediendienste-Staatsvertrag.

Seither wurden der Dienststelle mehrfach neue Aufgaben zugewiesen. Im November 1992 wurde der *Landesbeauftragte zur Aufarbeitung der Unterlagen des Staatssicherheitdienstes der ehemaligen Deutschen Demokratischen Republik* im Land Berlin in unserem Geschäftsbereich eingerichtet, wenn auch in fachlicher Unabhängigkeit. Im Juli 1995 wurde der Berliner Datenschutzbeauftragte aufgrund einer Gesetzesänderung auch *Aufsichtsbehörde* für den privaten Bereich, im gleichen Jahr wurde das Amt in der Berliner Verfassung verankert (Art. 47).

Mit dem Berliner *Informationsfreiheitsgesetz* vom 15. Oktober 1999 wurde der Berliner Datenschutzbeauftragte auch mit der Aufgabe der Wahrung des Rechts auf Akteneinsicht und Informationszugang betraut. Seither führt er in Anlehnung an die brandenburgische Regelung die Amtsbezeichnung „Berliner Beauftragter für den Datenschutz und für das Recht auf Akteneinsicht“, die von uns für den Alltags-

gebrauch auf „Berliner Beauftragter für Datenschutz und Akteneinsicht“ (BlnBDA) verkürzt wurde. Erst nach einigen Monaten wird erkennbar sein, welche Aufgaben damit auf uns zukommen und wie diese die Aufgabenstellung beeinflussen werden.

Das 20-jährige Bestehen der Dienststelle, das zusammen mit Dr. Kerkau, Mitgliedern des Abgeordnetenhauses und der Berliner Verwaltung, den derzeitigen und ehemaligen Mitarbeiterinnen und Mitarbeitern sowie vielen Helfern aus den ganzen Jahren zuvor in einer kleinen Feierstunde begangen worden war, wurde am 27. November 1999 zum Anlass für einen *Tag der offenen Tür* genommen. Viele Interessierte konnten sich über die Vielgestaltigkeit unserer Arbeit informieren; in kleinen Vorträgen und Einzelberatungen präsentierten die Referentinnen und Referenten ihr jeweiliges Arbeitsgebiet. Der Tag wurde damit eingeleitet, dass der gerade gewählte neue *Präsident des Abgeordnetenhauses* Reinhard Führer das Türschild mit der neuen Amtsbezeichnung am Dienstgebäude in der Pallasstr. 25 in Schöneberg anbrachte. Er betonte in seiner Ansprache die Bedeutung des Datenschutzes gerade in den Zeiten des Internet.

6.2 Die Aufgaben

Die Anzahl der Vorgänge, die im vergangenen Jahr zu bearbeiten waren, stieg erneut an. Deutlich erkennbar ist, dass die Bürgerinnen und Bürger sich zunehmend um den Schutz ihrer Daten in den elektronischen Medien sorgen. Dies wird durch Umfrageergebnisse im In- und Ausland bestätigt, die einhellig zeigen, dass zwei Drittel und mehr aller Befragten den Datenschutz zu den großen Problembereichen der Gegenwart zählen. Auf der anderen Seite nimmt auch die Anzahl der Personen und Stellen, die uns ihre Anliegen über *E-Mail* übersenden, stark zu.

Bei den einzelnen Lebensbereichen, aus denen die *Beschwerden* kommen, gab es eine deutliche Verschiebung hin zur Privatwirtschaft, gegen die sich inzwischen nahezu die Hälfte aller Eingaben richtet. Innerhalb der öffentlichen Verwaltung stehen wiederum wie in den Vorjahren die Bereiche Inneres und Gesundheit/Soziales gleichauf an der Spitze, gefolgt von Justiz und Bildung – es ist erstaunlich, wie konstant die Rangfolge über die Jahre hinweg geblieben ist.

Bei den *Beratungsersuchen* stehen andere Gebiete im Vordergrund: Hier kommen die meisten Anfragen aus dem Bereich Forschung und Bildung, gefolgt von Arbeitnehmerdaten (insbesondere Beratung von Betriebs- und Personalräten) und Gesundheit/Soziales.

Im abgelaufenen Jahr wurden im Rahmen der bisher nach dem BDSG nur bei Datenverarbeitung für fremde Zwecke möglichen *Amtskontrolle* Überprüfungen auf folgenden Arbeitsgebieten durchgeführt: Datenträgervernichtung, Rechenzentren-Betrieb, Lohn- und Gehalts-

abrechnung, Detekteien, Sachverständigen- bzw. Dienstleistungsbüros, Mikroverfilmung, Auskunfteien. Naturgemäß war der Umfang dieser Kontrollen sehr unterschiedlich, da er stark von Größe und Geschäftstätigkeiten der Unternehmen abhängt. So betrug der Kontrollaufwand für kleine Firmen mitunter nur wenige Stunden, während die Kontrolle eines großen Datenverarbeitungsdienstleisters über drei Tage lang von mehreren Kontrollteams und mit großem Vor- und Nachbereitungsaufwand stattfand.

Im Ergebnis ist festzustellen, dass dem *Datenschutz im privaten Bereich* große Aufmerksamkeit beigemessen wird. Insbesondere Firmen, die mit der Bewirtschaftung von Geldmitteln befasst sind (z. B. Lohn- und Gehaltsabrechnungsbüros), haben einen hohen Sicherheitsstandard, der auch dem Umgang mit personenbezogenen Daten zugute kommt. Auch dort, wo besonders sensible Daten verarbeitet werden, z. B. bei privatärztlichen Abrechnungsstellen, wird dem Datenschutz besondere Aufmerksamkeit gewidmet. Das Eigeninteresse an der ordnungsgemäßen Abwicklung der Auftragsarbeiten und die Gefahr, bei Nichteinhaltung der vertraglichen Vereinbarungen den Auftrag zu verlieren, sind oft auch Motor für die Beachtung der Datenschutzvorschriften. Offensichtlich schlagen Sicherheitsmängel, die zu Schäden und wirtschaftlichen Einbußen führen, bei Privatunternehmen direkter auf die persönlichen Karrieren, vielfach auch auf die wirtschaftliche Existenz der Verantwortungsträger durch.

Natürlich gibt es immer auch Ausnahmen von der Regel. So wurde ein Unternehmen vorgefunden, bei dem die datenschutzrechtlichen Bestimmungen, zu denen in diesem Fall auch die Regelungen der ärztlichen Schweigepflicht gehörten, offenbar noch nicht richtig bekannt waren. Von der Unterbringung hochsensibler medizinischer Befunde und Diagnosen bis hin zur organisatorischen Realisierung der Fernwartung reichte die Mängelliste dieser Stelle.

Dagegen haben wir bei einem führenden Dienstleister im Bereich der Datenverarbeitung in den von uns kontrollierten Teilbereichen ein Sicherheitsniveau festgestellt, welches in der mittlerweile zwanzigjährigen Kontrollpraxis unseres Hauses kaum eine Parallele gefunden hat.

6.3 Zusammenarbeit mit dem Abgeordnetenhaus

Wie im Vorjahr beschlossen[200] wurden die Ergebnisse der Arbeiten im *Unterausschuss „Datenschutz“* des Abgeordnetenhauses erstmals im Plenum beraten. Dies geschah diesmal gleichzeitig mit der Einbringung des Jahresberichtes 1998 sowie der Senatsstellungnahme hierzu in der Sitzung vom 1. Juli 1999; wie jedes Jahr machte der Berliner Daten-

200 vgl. JB 1998 6.3

schutzbeauftragte dabei von seinem Rederecht Gebrauch[201]. Er dankte dabei vor allem für die konstruktive Zusammenarbeit im Unterausschuss unter dem Vorsitz des Abgeordneten Rüdiger Jakesch. Bis zum Ende der Legislaturperiode hatte der Unterausschuss insgesamt 35mal getagt, wobei neben den jeweiligen Jahresberichten auch eine Vielzahl aktueller Datenschutzprobleme erörtert wurde.

Als Ergebnis der Beratungen zum Jahresbericht 1997 fasste das *Abgeordnetenhaus* nach dem Vorbild des Deutschen Bundestages einen Beschluss, in dem die Verwaltung in 15 einzelnen Punkten zur Verbesserung des Datenschutzes aufgefordert wurde[202].

6.4 Kooperation mit anderen Datenschutzstellen

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 24 Abs. 4 BlnDSG). In der *Konferenz* der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr unter dem Vorsitz des Landesbeauftragten von Mecklenburg-Vorpommern Dr. Werner Kessel in Schwerin (57. Konferenz am 25./26. März) und Rostock (58. Konferenz am 7./8. Oktober) tagte, wurde wiederum eine Reihe von Beschlüssen gefasst, die in besonderer Weise der Fortentwicklung des Datenschutzes dienen. Die Ergebnisse sind bei den Berichten aus den Arbeitsgebieten dargestellt worden. Im laufenden Jahr hat der Niedersächsische Datenschutzbeauftragte Burckardt Nedden den Vorsitz übernommen.

Bereits 1998 hatten die Landesbeauftragten von Brandenburg, Bremen, Nordrhein-Westfalen, Schleswig-Holstein und Berlin gemeinsam eine neue Datenschutzpolitik gefordert[203]. Im vergangenen Jahr wurde diese besondere Zusammenarbeit mit der Veröffentlichung von Thesen zur Sicherung der freien Telekommunikation in unserer Gesellschaft fortgesetzt[204].

Wie in den Vorjahren war die Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg bei gemeinsamen Einrichtungen, aber auch bei Problemen, die von gemeinsamem Interesse sind, besonders intensiv. Bei regelmäßigen Treffen auf Leitungsebene wurden darüber hinaus Absprachen über die Vertiefung der Kooperation, z. B. durch Informationen über die bearbeiteten Vorgänge sowie durch gemeinsame Prüfungen, getroffen. Am Tag der offenen Tür beteiligte sich die brandenburgische Dienststelle mit einer eigenen Präsentation.

---

201 Anlage 1
202 Anlage 2
203 10 Punkte für einen Politikwechsel zum wirksameren Schutz der Privatsphäre, JB 1998, Anlagenband „Dokumente zum Datenschutz 1998“, Teil A
204 Anlagenband „Dokumente zum Datenschutz 1999“, Teil B

Für den Bereich der Aufsicht von Privatunternehmen wird die Koordinierung im *„Düsseldorfer Kreis“,* dem Gremium der Obersten Aufsichtsbehörden für den Datenschutz, wahrgenommen, der sich ebenfalls zweimal im Jahr unter Vorsitz des nordrhein-westfälischen Innenministeriums trifft. Auch hier nehmen wir aktiv teil, in zwei Arbeitsgruppen – Teledienste und Telekommunikation[205] sowie Internationaler Datenverkehr[206] – führt der Berliner Beauftragte für Datenschutz und Akteneinsicht den Vorsitz.

Die Zusammenarbeit zwischen den beiden Gremien, die wegen der Vielzahl gemeinsamer Probleme nicht nur sinnvoll, sondern sogar notwendig wäre, wird seit Beginn nur bilateral in den Ländern, nicht jedoch gemeinsam wahrgenommen – mit Ausnahme natürlich derjenigen Länder, in denen private und öffentliche Kontrolle vereint sind (außer Berlin noch Bremen, Hamburg, Niedersachsen und demnächst – wieder – Schleswig-Holstein). Eine Ausnahme bildet auch hier der Bereich der Telekommunikation und der Teledienste. In Berlin wurde 1997 ein gemeinsamer *Kooperationskreis IuK-Datenschutz* gegründet, dessen Aufgabe in der Koordinierung der Kontrolltätigkeit bei Tele- und Mediendiensten besteht und der im vergangenen Jahr eine Sitzung in Berlin abhielt.

Die Zusammenarbeit auf europäischer Ebene wird immer wichtiger. Berlin hat hier mit der Arbeitsgruppe Internationaler Datenverkehr des „Düsseldorfer Kreises“ eine besondere Aufgabe übernommen. Mit dem Ausscheiden des Bremischen Landesbeauftragten Dr. Stefan Walz wird der Berliner Beauftrage für Datenschutz und Akteneinsicht als stellvertretender Delegationsleiter die deutschen Landesbeauftragten in der *Gruppe nach Art. 29* der europäischen Richtlinie vertreten. Der dringende Wunsch der Europäischen Kommission, dass wir uns aufgrund unserer Sachkompetenz intensiv in der Internet Task Force der Gruppe engagieren, kann leider bisher mangels hinreichender Arbeitskapazitäten nicht erfüllt werden.

Die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation tagte unter Berliner Vorsitz zweimal, vom 26. bis 29. April auf Einladung der Dateninspektion in Norwegen sowie am 31. August in Berlin. Traditionsgemäß nahmen die Mitglieder am 30. August an einem Internationalen Symposium anlässlich der Internationalen Funkausstellung teil, das diesmal unter dem Thema „Datenschutz – Brücke zwischen Privatheit und Weltmarkt“ stand. Vertreter verschiedenster Institutionen und Unternehmen (OECD, DaimlerChrysler, Bertelsmann, Universität Freiburg) aus dem In- und Ausland (USA, Frankreich, Indien) stellten die Perspektiven von Datenschutz und Informationssicherheit im Zeitalter des entstehenden globalen elektronischen Mark-

205 vgl. 5.
206 vgl. 4.7

tes dar. Die Ergebnisse der Arbeitsgruppe[207] wurden mit großem Interesse auf der Internationalen Konferenz der Datenschutzbeauftragten am 13. bis 15. September in Hong Kong aufgenommen.

Im Rahmen unserer Aufgaben zum Internationalen Datenverkehr nehmen wir seit Jahren an einer deutsch-amerikanischen Arbeitsgruppe teil, die von einem der Väter der Datenschutzdiskussion in den USA, dem ehemaligen Professor an der Columbia-Universität New York, Alan Westin[208], dem für den BahnCard-Vertrag maßgeblichen Manager der Citibank, Duncan MacDonald, sowie dem Leiter des American Institute for Contemporary German Studies, Jack Janes, initiiert wurde. Ziel ist die Erarbeitung eines Mustervertrages (model contract), der ein angemessenes Datenschutzniveau in Drittländern sicherstellen soll[209].

6.5 Öffentlichkeitsarbeit

Mehr und mehr rückt das *Internet* in den Mittelpunkt unserer *Öffentlichkeitsarbeit*. Zwar werden die von uns herausgegebenen Materialien – von den Jahresberichten über die wichtigsten Gesetzestexte (zum Schutz der Sozialdaten wurde eine aktualisierte Zusammenstellung der Gesetze herausgebracht) bis hin zu der bewährten Materialienreihe – noch in Papierform verteilt. Auch das beliebte Datenscheckheft wurde neu aufgelegt.

Das Interesse, das diese papierenen Unterlagen finden, bleibt jedoch weit hinter den Anfragen zurück, die uns inzwischen über unsere Website www.datenschutz-berlin.de erreichen. So wurden die von uns herausgegebenen und im Netz zur Verfügung gehaltenen Broschüren pro Monat im Durchschnitt allein 1 800-mal heruntergeladen, d.h. nicht nur gelesen, sondern auch auf den heimischen Computer geholt. Das entspricht einer Auflage, die wir auf herkömmliche Weise nie erreicht haben. Dies ist auch der Grund, weshalb wir darüber nachdenken, die herkömmlichen Publikationen wenigstens zum Teil durch *Online-Publikationen* zu ersetzen. Interessierte, die selbst nicht über einen Internetanschluss verfügen, können dabei alle Texte, die im Internet präsent sind, aber auch andere Texte, die uns zur Verfügung stehen, in aktueller, frisch ausgedruckter, aber gleichwohl ansprechender Form bei uns abrufen.

Erheblich eindrucksvoller als die Zahl der downloads ist diejenige der Internetseiten, die nur gelesen werden. Ende 1999 wurden ca. 100 000 Seitenabrufe pro Monat gezählt (eine Seite entspricht häufig mehreren Druckseiten), die Zahl der übertragenen Dateien („hits“) liegt bei 300 000 im Monat. Nicht mitgezählt sind hier natürlich alle Dokumente,

---

207 vgl. 5.1

208 sein Buch Privacy and Freedom, New York 1967, beeinflusste maßgeblich die amerikanische Gesetzgebung zum Datenschutz (privacy)

209 vgl. 4.7

die nicht von unserem Server, sondern von Proxiservern etwa in den Universitäten abgerufen werden. Hinzu kommen noch alle Abrufe im Berliner Landesnetz, in das monatlich die neueste Version unseres Webangebots eingespielt wird.

Besonders beliebt bei den Abrufen ist die tägliche Presseschau „Prima“ *(privacy magazine)*, die bei vielen behördlichen und betrieblichen Datenschutzbeauftragten (übrigens auch im Ausland) zur täglichen Lektüre gehört.

Als wichtigste Neuerung wurde pünktlich zum Tag der offenen Tür eine *Suchmaschine* über die Webangebote aller Landesbeauftragten und des Bundesbeauftragten für den Datenschutz eingerichtet. Der der Suche zugrunde liegende Index wird täglich neu aufgebaut, so dass – im Gegensatz zur Suche über kommerzielle Dienste – auch aktuelle Änderungen und Ergänzungen auffindbar sind.

Gerade beim Internet bietet sich eine Zusammenarbeit der Datenschutzbeauftragten besonders an, um Doppelarbeit zu vermeiden. So wird sich Berlin an einer Initiative des Landesbeauftragten von Schleswig-Holstein beteiligen, der unter dem Titel *„Virtuelles Datenschutzbüro“* eine neue Form des Bürgerservice zum Datenschutz initiiert hat. Auf diese Weise wird es wenigstens in der virtuellen Welt eine Aufhebung der Zersplitterung des Datenschutzes geben, die zu beseitigen in der realen Welt bislang nicht gelungen ist.

Berlin, 2. März 2000

Prof. Dr. Hansjürgen Garstka

Berliner Beauftragter für
Datenschutz und Akteneinsicht

Rede des Berliner Datenschutzbeauftragten am 1. Juli 1999 im Abgeordnetenhaus zur Einbringung des Jahresberichts 1998 sowie zur Beschlussfassung über den Jahresbericht 1997

„Herr Präsident, sehr geehrte Damen und Herren,

der Datenschutz erhält heute im Plenum dieses Hauses einen neuen Stellenwert: Erstmals wird nicht nur der Tätigkeitsbericht des Datenschutzbeauftragten zum Vorjahr formal eingebracht, sondern es liegen auch die Ergebnisse der Beratung zum Tätigkeitsbericht 1997 zur Beschlussfassung vor. Dies gibt – wenn auch in engem zeitlichem Rahmen – die Gelegenheit, einige wesentliche Themen anzusprechen, die der parlamentarischen Behandlung bedurften und nach Zustimmung des Abgeordnetenhauses dem Datenschutz in der öffentlichen Verwaltung Berlins entscheidenden Nachdruck verleihen werden.

Die Themen, die der Unterausschuss „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung beraten hat, repräsentieren wie in einem Brennglas Probleme, die die Datenschutzdiskussion seit nunmehr fast 20 Jahren geprägt haben. Die Notwendigkeit einer parlamentarischen Debatte zeigt, dass der Datenschutz zwar in der Berliner Verwaltung ein anerkanntes Regelungsziel ist, diesem in der Praxis jedoch nicht immer eine angemessene Bedeutung beigemessen wird.

Die vordergründigste Aufgabe des Datenschutzes ist der Schutz personenbezogener Daten vor unbefugter Kenntnisnahme: Neben den immer wieder vorkommenden Nachlässigkeiten im Umgang mit den Daten bergen bestimmte Organisationsformen das Risiko unberechtigter Zugriffe: Etwa die Beschäftigung von Sozialhilfeempfängern mit Tätigkeiten, bei denen diese ihrerseits Sozialdaten zur Kenntnis nehmen können, oder das immer stärker eingesetzte „Outsourcing“ bei der Verarbeitung sensibler Daten, das am Beispiel der Vergabe der Krankenaktenarchivierung eines ganzen Klinikums an ein Privatunternehmen diskutiert wurde.

Neben dem Schutz vor unbefugter Kenntnisnahme ist der Schutz der Bürgerinnen und Bürger vor der Verwertung veralteter Daten ein zentrales Ziel des Datenschutzes: Das Recht einer jeden Person auf Rehabilitation und Neuanfang muss abgesichert werden durch die fristgerechte Löschung von Daten über Verfehlungen, vergleichbar mit der menschlichen Tugend des Vergessens und Vergebens. Dies den Ordnungsbehörden immer wieder nahe zu legen, ist eine unserer wichtigsten Aufgaben. Parlamentarischer Unterstützung bedurfte es bei der Umsetzung neuer Vorschriften im Straßenverkehrsrecht, die die von dem Datenschutzbeauftragten seit vielen Jahren geforderte Bereinigung der Führerscheinakten von weit zurückliegenden Straftaten zur

gesetzlichen Pflicht machen, oder bei der Frage, wie lange längst veraltete Bundeszentralregisterauskünfte in den Gewerbeakten aufbewahrt werden dürfen.

Das Bundesverfassungsgericht hat dem Datenschutz in der Form des informationellen Selbstbestimmungsrechtes Grundrechtscharakter verliehen; daraus folgt, dass – soweit möglich – die ohne Zwang ausgesprochene Einwilligung der Betroffenen in die Verarbeitung ihrer Daten oberster Grundsatz sein sollte. Gerade die Nutzung neuer Informationstechnik, die mit großen Risiken verbunden ist, bedarf grundsätzlich der freien Entscheidung der Betroffenen. Die Veröffentlichung von Personaldaten im Internet oder die Veröffentlichung von Daten über Mitarbeiterinnen und Mitarbeiter der Verwaltung, die im Rahmen des „Ideenmanagements“ Vorschläge für die Verbesserung von Arbeitsabläufen machen, sind Beispiele hierfür.

Die Gesetzgebung auf dem Gebiet des Datenschutzes wird häufig sehr kritisch betrachtet, im vergangenen Herbst etwa in den Diskussionen des Deutschen Juristentags in Bremen. Der Vorwurf der Überregulierung ist jedoch unberechtigt. An manchen Stellen mag der Gesetzgeber zwar über das gebotene Maß an Regulierung hinausgeschossen sein. In der Regel geschah dies aber gerade nicht, um Bürgerrechte zu schützen, sondern um immer weiter gehende Eingriffe in die informationelle Selbstbestimmung zu ermöglichen.Demgegenüber gibt es noch immer Bereiche, in denen konkrete Datenschutzregelungen, die dem Bürger Rechte in die Hand geben, fast ganz fehlen oder die diese Rechte nicht hinreichend klar berücksichtigen. So verschafft das Steuerrecht dem Staat zwar außer Geld den Zugang zu einer Vielzahl sensibelster Daten, enthält aber nach wie vor den Steuerzahlern das in anderen Gebieten selbstverständliche Recht auf Auskunft über ihre Daten vor. Die Beschlussempfehlung, der Senat solle sich für die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung einsetzen, zielt auf die Schließung einer der letzten großen Lücken der Datenschutzgesetzgebung.

Andere Bereiche, wie z. B. das Melderecht, warten seit Jahren auf datenschutzrechtliche Korrekturen.

Das Bundesverfassungsgericht hat die Existenz der Datenschutzbeauftragten als eine unabdingbare Voraussetzung des rechtmäßigen Umgangs mit personenbezogenen Daten angesehen. Voraussetzung hierfür ist der unbeschränkte und bedingungslose Zugang des Datenschutzbeauftragten zu den Daten sowie den Unterlagen über ihre Verarbeitung. Vor diesem Hintergrund verwundert es, dass es eines Beschlusses dieses Hauses bedarf, um die Innenverwaltung anzumahnen, den Datenschutzbeauftragten auch rechtzeitig über datenschutzrelevante Vorhaben des Bundes zu informieren, die für die Verarbeitung von Daten in den Ländern von großer Bedeutung sind. Überhaupt ist in einigen Bereichen die Bereitschaft der Verwaltung, mit dem Daten-

schutzbeauftragten zu kooperieren, in den letzten Jahren deutlich gesunken, so dass in jüngster Zeit sogar der Eindruck entstand, der Datenschutz solle aus politischen Diskussionen herausgehalten werden.

Weltweit wird heute unter dem Schlagwort „Privacy Enhancing Technologies“ die Forderung diskutiert, dass Datenschutz nicht nur als lästiges Anhängsel von Automationsvorhaben, sondern als Strukturmerkmal informationstechnischer Verfahren betrachtet wird. In den Beschlussentwürfen, die Ihnen zur Einführung von Informations-, Kommunikations- und Mediendiensten durch öffentliche Wohnungsbaugesellschaften, zu der Neugestaltung des polizeilichen Informationssystems oder zur Landesinitiative „Der Berliner Weg in die Informationsgesellschaft“ vorliegen, macht sich dieses Haus die Forderung nach datenschutzfreundlichen Technologien zu eigen. Es sollte Ziel Berliner Politik sein, diese Stadt nicht nur zu einem hervorragenden Standort für Informations- und Kommunikationstechnik zu machen, sondern auch Vorbild zu geben für die menschengerechte Gestaltung dieser Techniken. Dass dabei Grenzen des Einsatzes der Informationstechnik ins Blickfeld geraten, zeigen die in Berlin wohl inzwischen fallen gelassenen Pläne zur Einführung einer Elektronischen Fußfessel, die den Strafvollzug durch einen virtuellen elektronischen Käfig ersetzt.

Der Jahresbericht 1998 zeigt erneut, dass die Informationstechnik und damit die daraus resultierenden Datenschutzprobleme für die Menschen immer undurchschaubarer werden. Umso unverständlicher ist es, dass der Datenschutz zu denjenigen Gebieten gehört, die man (angesichts organisatorischer und haushaltsmäßiger Zwänge) am ehesten vernachlässigen zu können glaubt – unsere Untersuchung zu Stellung und Unterstützung behördlicher Datenschutzbeauftragter in der Berliner Verwaltung macht dies deutlich.

Ich bin mir sicher, dass wir auch zu den für das Jahr 1998 angesprochenen Problemen die Unterstützung dieses Hauses erfahren werden, wie dies in den vergangenen Jahren im Unterausschuss „Datenschutz“ unter seinem Vorsitzenden Rüdiger Jakesch der Fall war und wofür ich mich an dieser Stelle sehr bedanken möchte.

Anlage 1

Ergebnisse der Beratungen des Unterausschusses „Datenschutz“

Beschluss des Abgeordnetenhauses von Berlin vom 1. Juli 1999 zu:

Stellungnahme und Beschlussempfehlung
des Ausschusses für Inneres, Sicherheit und Ordnung vom 14. Juni 1999
zur Vorlage

über Stellungnahme des Senats zum Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1997
– Drs. 13/2918, 13/3840 –

Das Abgeordnetenhaus von Berlin hat in seiner 51. Sitzung am 1. Oktober 1998 die Vorlage – zur Kenntnisnahme – über Stellungnahme des Senats zum Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1997 – Drs. 13/2918 – ohne Aussprache zur Besprechung an den Ausschuss für Inneres, Sicherheit und Ordnung, überwiesen. In der Ältestenratssitzung am 29. September 1998 war diese Überweisung mit der Bitte um Abgabe einer Stellungnahme an das Plenum mit einem Besprechungsvorbehalt zu einem späteren Zeitpunkt empfohlen worden.

Der Ausschuss für Inneres, Sicherheit und Ordnung hat diese Vorlage am 9. November 1998 zur Besprechung an den Unterausschuss Datenschutz überwiesen, der in mehreren Sitzungen die Vorlage und den Bericht beraten hat. Mit Schreiben vom 29. April 1999 legte dieser eine abschließende Stellungnahme vor. Diese hat sich der Ausschuss für Inneres, Sicherheit und Ordnung in seiner 66. Sitzung am 14. Juni 1999 zu Eigen gemacht.

Der Ausschuss empfiehlt entsprechend der Verfahrensweise im Deutschen Bundestag bei den Beratungen der Berichte des Bundesbeauftragten für den Datenschutz, dass das Ergebnis seiner Beratung in einen Beschluss des Abgeordnetenhauses mündet.

Insofern wolle das Abgeordnetenhaus zu den einzelnen Textziffern des Berichts des Berliner Datenschutzbeauftragten auf der Grundlage der Drucksache 13/2918 beschließen:

1. Tz 4.2.3. „Straßenverkehrsgesetz“

(Umsetzung der neuen, ab 1. Januar 1999 geltenden Bestimmungen des Straßenverkehrsgesetzes über Vernichtungsfristen, S. 65)

„Der Senat wird aufgefordert dafür Sorge zu tragen, dass die Bereinigung der Führerscheinakten nach den ab 1. Januar 1999 geltenden

neuen Bestimmungen des Straßenverkehrsgesetzes und der hierzu erlassenen Arbeitsanweisung möglichst frühzeitig abgeschlossen wird."

2. Tz 4.4.4. „Wohnen" („Sitzt der Vermieter bald mit auf dem Sofa?")

(Voraussetzungen für den Einsatz von Fernmessdiensten bei Wohnungsbaugesellschaften, S. 91)

„Der Senat wird aufgefordert, bei den Siedlungs- und Wohnungsbaugesellschaften des Landes Berlin darauf hinzuwirken, ferngesteuerte Messungen und Beobachtungen in Wohnungen oder Geschäftsräumen nach § 31 a Berliner Datenschutzgesetz nur dann vorzunehmen, wenn die Betroffenen zuvor umfassend über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes der Dienste unterrichtet worden sind und darin schriftlich eingewilligt haben.

Bei der Einführung von Informations- und Kommunikationsdiensten sowie von Mediendiensten sind darüber hinaus die datenschutzrechtlichen Bestimmungen des Teledienstedatenschutzgesetzes bzw. des Mediendienste-Staatsvertrages zu beachten.

Der Senat soll darauf hinwirken, dass die Wohnungsbaugesellschaften des Landes Berlin die Verfahren so ausgestalten, dass eine anonyme Nutzung von Informations- und Kommunikationsdiensten ermöglicht wird."

3. Tz 4.3.2 „Finanzen"

(Einsatz des Senats für Datenschutzregelungen in der Abgabenordnung, S. 72)

„Die Regelungen des Steuergeheimnisses stellen den Datenschutz im Anwendungsbereich der Abgabenordnung nicht in dem vom Bundesverfassungsgericht im Volkszählungsurteil vorgegebenen Umfang sicher. Der Senat wird daher aufgefordert, sich auf Bundesebene für die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung einzusetzen."

4. Tz 3.1. „Der Bürger im Netz der Sozialdatenverarbeitung"

(Datenabgleich im Sozialwesen, Erfolgskontrolle, S. 24)

„Die Senatsverwaltung für Gesundheit und Soziales wird aufgefordert, dem Unterausschuss „Datenschutz" zu berichten, zu welchen Ergebnissen der bundesweite und innerhalb des Landes Berlin zwischen Sozialbehörden und anderen Behörden durchgeführte Datenabgleich zur Bekämpfung des Leistungsmissbrauchs im Sozialhilfewesen geführt hat."

5. Tz 4.4.3. (Sozialverwaltung)

(Gemeinnützige Arbeit von Sozialhilfeempfängern in Bereichen, in denen personenbezogene Daten anfallen, S. 87)

„Das Abgeordnetenhaus fordert die Senatsverwaltung für Gesundheit und Soziales auf, in einem Rundschreiben an die Bezirksämter die Kriterien vorzugeben, nach denen sichergestellt ist, dass Sozialhilfempfängern bei gemeinnützigen Tätigkeiten nach § 19 BSHG keine schutzwürdigen personenbezogenen Daten zur Kenntnis gelangen.

Der Entwurf des Rundschreibens ist mit dem Berliner Datenschutzbeauftragten abzustimmen und dem Unterausschuss „Datenschutz“ zur Kenntnis zu geben.“

6. Tz 4.4.2. „Gesundheit“(Krankengeschichten in fremden Händen)

(Archivierung von Krankengeschichten durch Privatunternehmen, S. 85)

„Das Abgeordnetenhaus unterstützt die Auffassung des Berliner Datenschutzbeauftragten und der Senatsverwaltung für Gesundheit und Soziales, dass Krankengeschichten und Patientendaten auch beim Einsatz externer Firmen nicht aus dem Verfügungs- und Verantwortungsbereich des Krankenhauses oder des Arztes herausgenommen werden dürfen.“

7. Tz 4.1.1. „Polizei“ (Errichtungsanordnung für AFIS)

(Information des Datenschutzbeauftragten über Gesetzesvorhaben, Verwaltungsvorschriften, Errichtungsanordnungen u.a. des Bundes, S. 48)

„Das Abgeordnetenhaus spricht sich dafür aus, dass es zur Unterstützungspflicht der öffentlichen Stellen nach § 28 Berliner Datenschutzgesetz gehört, den Berliner Datenschutzbeauftragten auch rechtzeitig über datenschutzrelevante Vorhaben auf Bundesebene, an denen die Länder beteiligt werden (einschl. Verwaltungsvorschriften wie Errichtungsanordnungen), zu unterrichten, damit seine Empfehlungen bei Abgabe der Stellungnahme berücksichtigt werden können.“

8. Tz 4.1.1 „Polizei“ (Der Abgehörte Anwalt in der Wahllichtbildvorlage)

(Verteilung der datenschutzrechtlichen Verantwortung zwischen der Senatsverwaltung für Inneres und der Senatsverwaltung für Justiz, S. 50)

„Das Abgeordnetenhaus stellt fest, dass die Polizei für die von ihr im Rahmen von Strafermittlungsverfahren erhobenen, gespeicherten und übermittelten personenbezogenen Daten verantwortliche Daten ver-

arbeitende Stelle und die Senatsverwaltung für Inneres Beanstandungsadressat nach § 26 Abs. 1 Berliner Datenschutzgesetz im Einvernehmen mit der Senatsverwaltung für Justiz ist.

Der Senat wird aufgefordert, seine bislang nicht vorliegende Stellungnahme hierzu umgehend vorzulegen."

9. Tz 4.2.1. „Meldewesen und Wahlen"

(Novellierung des Meldegesetzes, S. 59)

„Die Senatsverwaltung für Inneres wird aufgefordert, einen Entwurf zur Novellierung des Meldegesetzes vorzulegen, der die durch das Melderechtsrahmengesetz in der Fassung vom 11. März 1994 gebotenen Änderungen sowie weitere Vorschläge zur Verbesserung des Datenschutzes berücksichtigt."

10. Tz 4.4.1 „Arbeitnehmer und öffentliche Bedienstete" (Unsensibel mit sensiblen Daten)

(Offenbarung personenbezogener Daten im Vorschlagswesen, S. 80)

„Der Senat wird aufgefordert sicherzustellen, dass Verbesserungsvorschläge im Rahmen des „Berliner Ideenmanagement" grundsätzlich vertraulich behandelt und nur dann personenbezogen an Dritte weitergegeben oder veröffentlicht werden, wenn der Beschäftigte in die Nennung seines Namens einwilligt."

11. Tz 2.3. „Datenverarbeitung in Berlin" und Tz 4.7.3. „Telekommunikation in der Berliner Verwaltung"

(Internetnutzung in der Berliner Verwaltung, S. 19 und S. 122)

„Die öffentlichen Stellen des Landes Berlin werden aufgefordert, Internet-Dienste am Arbeitsplatz nur dann zu nutzen, wenn ein wirksames Sicherheitskonzept erarbeitet und geeignete Sicherheitsmaßnahmen getroffen wurden. Die Vorgaben der IT-Sicherheitsrichtlinie sind zu beachten. Die öffentlichen Stellen des Landes Berlin werden weiterhin aufgefordert, Daten von Arbeitnehmern ohne Einwilligung in öffentliche elektronische Verzeichnisse nur aufzunehmen, soweit hierfür eine arbeitsvertragliche Notwendigkeit besteht."

12. Tz 2.3. „Datenverarbeitung in Berlin"

(Erneuerung des polizeilichen Informationssystems, S. 24)

„Der Senat wird aufgefordert, bei der Erneuerung des polizeilichen Informationssystems die in den vergangenen Jahren erhobenen datenschutzrechtlichen Anforderungen (z. B. Trennung des Zugriffs auf Daten Verdächtiger und anderer Personen) zu berücksichtigen. Der Berliner Datenschutzbeauftragte ist rechtzeitig in die Planungen einzubeziehen."

13. Tz 4.3.1. „Justiz“ (Elektronisch überwachter Hausarrest – eine neue Form des Strafvollzugs)

(Einführung des „elektronischen Hausarrests“, S. 69)

„Die Senatsverwaltung für Justiz wird aufgefordert, den Abschlussbericht der länderübergreifenden Arbeitsgruppe, die sich unter der Federführung Berlins umfassend mit den Fragen des elektronisch überwachten Hausarrests befasst hat, unmittelbar nach dessen Fertigstellung dem Unterausschuss „Datenschutz“ und dem Berliner Datenschutzbeauftragten zur Verfügung zu stellen.“

14. Tz 2.3. „Datenverarbeitung in Berlin“

(Berücksichtigung des Datenschutzes bei der Landesinitiative „Der Berliner Weg in die Informationsgesellschaft“, S. 19)

„Die Senatsverwaltung für Wirtschaft und Betriebe wird aufgefordert, sich dafür einzusetzen, dass bei der Entwicklung von Projekten im Rahmen der Landesinitiative „Der Berliner Weg in die Informationsgesellschaft“ datenschutzfreundliche Technologien berücksichtigt werden. Das Prinzip der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen ist zu verwirklichen. Der Berliner Datenschutzbeauftragte ist rechtzeitig über die Entwicklung der Projekte zu unterrichten.“

15. Tz 4.2.4. „Wirtschaftsverwaltung“ (Datenlöschung in Gewerbeakten)

(Bundeszentralregisterauszüge in Gewerbeakten, S. 66)

„Die Senatsverwaltung für Wirtschaft wird aufgefordert zu veranlassen, dass Bundeszentralregisterauszüge in Gewerbeakten, wenn sie für die Aufgabenerfüllung nicht mehr erforderlich sind, zu vernichten sind. Dies gilt auch für zu den Akten genommene Kopien von den den Bundeszentralregisterauszügen zugrunde liegenden Strafurteilen.“

Berlin, den 15. Juni 1999

Der Vorsitzende des Ausschusses für Inneres, Sicherheit und Ordnung

Rüdiger Jakesch

Anlage 2

Diskussionsgrundlage zur weiteren Verwendung von Stasi-Unterlagen zur Überprüfung von Mandatsträgern und Mitarbeitern im öffentlichen Dienst[1]

Im nächsten Jahr wird die Bundesrepublik Deutschland den 10. Jahrestag der Wiedervereinigung begehen. Mit Blick hierauf ist es an der Zeit, die Überprüfungen bei Mandatsträgern und Mitarbeitern im öffentlichen Dienst anhand von Stasi-Unterlagen zu überdenken und neu zu gestalten.

Personenbezogene Informationen dürfen nur verarbeitet werden, wenn sie rechtmäßig erhoben worden sind. Dies verlangt ein wesentlicher datenschutzrechtlicher Grundsatz unserer Verfassung. Deshalb dürfen öffentliche Stellen Datensammlungen, die auf rechtswidrige Weise und unter Verstoß gegen Menschenrechte zu Stande gekommen sind, grundsätzlich nicht verwenden. Die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR sind derartige Datensammlungen. Die letzte frei gewählte Volkskammer und anschließend der Bundesgesetzgeber sind aber aus gewichtigen Gründen der seinerzeit stark diskutierten Forderung, diese Aktensammlungen unbesehen zu vernichten, nicht gefolgt.

Inzwischen sind allerdings die Überlegungen und Zielsetzungen, die zu einer Legitimation der weiteren Verwendung der Informationen aus diesen Datensammlungen geführt haben, differenziert und mit etwas mehr Abstand zu betrachten. So ist fraglich, ob Daten aus diesen Sammlungen bei Personalmaßnahmen im öffentlichen Dienst der neuen Bundesländer weiterhin uneingeschränkt als prägendes Element für das Kriterium der persönlichen Eignung und damit der Zuverlässigkeit herangezogen werden können, während in den alten Bundesländern eine Regelüberprüfung schon lange nicht mehr stattfindet. Angesichts der ständigen Fluktuation ganzer Bevölkerungsteile zwischen den alten und den neuen Bundesländern dürfte eine solch unterschiedliche Handhabung als Ungleichbehandlung nicht mehr zu rechtfertigen sein. Bezweifelt werden muss auch, ob bei den heute weit über 10 Jahre zurückliegenden Ereignissen der Wahrheitsgehalt einzelner Daten noch annähernd überprüft werden kann und eine gerechte Bewertung der Ergebnisse in jedem Einzelfall noch möglich ist. Ferner darf der im demokratischen Rechtsstaat verankerte Resozialisierungsgedanke nicht außer Acht gelassen werden.

Andererseits darf aber gerade das in weiten Teilen der Bevölkerung der neuen Bundesländer ausgeprägte Gefühl für gerechtes Handeln des Staates nicht einer formalen Rechtsstaatlichkeit untergeordnet werden.

---

[1] Dieses Papier wird unterstützt vom Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, vom Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern und vom Berliner Beauftragten für Datenschutz und Akteneinsicht.

Insbesondere die verbreitete Sorge in der Bevölkerung, bald wieder alten Peinigern in neuen öffentlichen Ämtern gegenüberzusitzen, darf nicht als vernachlässigbar abgetan werden.

Wir halten deshalb eine breite Diskussion über diesen Problembereich in ganz Deutschland für geboten.

Umfang der Überprüfungen

Einer kritischen Sicht bedarf die Frage, welche Personengruppen 10 Jahre nach Auflösung des Ministeriums für Staatssicherheit noch in die Überprüfung einbezogen werden:

Die Überprüfung öffentlicher Bediensteter sowie von Bewerbern für den öffentlichen Dienst zielt darauf ab festzustellen, ob die Betroffenen die hierfür erforderliche persönliche Zuverlässigkeit besitzen und ob ein Festhalten am Arbeitsverhältnis unzumutbar erscheint (vgl. Einigungsvertrag Anlage 1, Kapitel XIX, Sachgebiet A, Abschnitt III, Nr. 1, Abs. 5).

Ist von vornherein auszuschließen, dass die Überprüfung Ergebnisse bringt, die unter diesen Gesichtspunkten für eine Kündigung oder einen Ausschluss des Bewerbers verwertbar sind, hat die Überprüfung zu unterbleiben. Dies ist nach der höchst richterlichen Rechtsprechung schon jetzt der Fall, wenn

- ein nach der Wiedervereinigung begonnenes Arbeitsverhältnis jahrelang unbeanstandet geblieben ist, der/die Bedienstete sich mithin bewährt hat;
- eine einzelfallbezogene Würdigung der gesamten Persönlichkeit ohnehin dazu führen würde, dass eine eventuell entdeckte Stasi-Verstrickung keine besonderen Maßnahmen rechtfertigen würde oder
- wegen des Alters der Person eine Verstrickung ausgeschlossen ist oder wegen des Zeitablaufs nicht mehr berücksichtigt werden könnte.

Berücksichtigt werden muss darüber hinaus die Wertigkeit der konkret besetzten oder zu besetzenden Positionen; grundsätzlich sollten die Überprüfungen auf Personen beschränkt werden, die eine herausragende Stellung einnehmen oder einnehmen sollen. Dies muss auch bei Personengruppen gelten, denen die Bevölkerung ein besonderes Vertrauen entgegenbringen muss (Polizei, Justiz, Bildungswesen). Von Überprüfungen aller Personen des öffentlichen Dienstes einzelner Bundesländer sollte danach abgesehnen werden.

Dahingegen können und sollten weiterhin Überprüfungen durchgeführt werden, wenn der konkrete Verdacht besteht, dass ein Sachverhalt vorliegt, der personelle Maßnahmen rechtfertigen würde.

Obwohl das Stasi-Unterlagen-Gesetz die Weitergabe von Daten zur Überprüfung nur „nach Maßgabe der dafür geltenden Vorschriften“ zulässt (§ 21 Abs. 1 Nr. 6), sind auf Bundes- wie auf Länderebene besondere Rechtsvorschriften zur Überprüfung nur zum Teil geschaffen worden. Da die auf einer derart ungesicherten Rechtslage durchgeführten Überprüfungen mit fortschreitender Zeit immer tiefere Eingriffe in die informationelle Selbstbestimmung darstellen, wird ihre Verhältnismäßigkeit und damit ihre Zulässigkeit immer fragwürdiger.

Besondere Probleme wirft die Überprüfung von Mandatsträgern auf. Zwar gilt sie in den neuen Bundesländern noch immer als vertrauensbildende Maßnahme. Gleichwohl zeigt sich gerade hier, dass das Aufdecken einer früheren Verbindung zum Ministerium für Staatssicherheit nicht zwangsläufig zu Konsequenzen führt. Deshalb muss auch bei Mandatsträgern die Überprüfung in absehbarer Zeit ein Ende finden, zumal den Überprüfungen in aller Regel nur eine formal-freiwillige Einwilligung zugrunde liegt.

Überprüft wurden in den vergangenen 10 Jahren nahezu ausschließlich Personen aus den neuen Bundesländern, obwohl nach Einschätzung des BSW ca. 20 000 bis 30 000 Bürgerinnen und Bürger der alten Bundesländer Stasi-verstrickt sind. Nach zehnjähriger unterschiedlicher Überprüfungspraxis muss das Ziel nunmehr ein möglichst einheitliches Vorgehen sein, das die Vorschläge dieser Entschließung berücksichtigt.

Nutzung von Daten im Rahmen der Überprüfungen

Die Nutzung von Daten im Rahmen von Überprüfungen muss sowohl dem Anliegen des Stasi-Unterlagen-Gesetzes (StUG), die historische, politische und juristische Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes zu gewährleisten und zu fördern, als auch dem Recht der Betroffenen auf informationelle Selbstbestimmung Rechnung tragen.

Es ist unvermeidbar, dass bei Recherchen zu Überprüfungen durch Mitarbeiter des Bundesbeauftragten für die Stasi-Unterlagen auch Unterlagen von Opfern des Staatssicherheitsdienstes eingesehen werden müssen. Dieser tiefe Eingriff in die Privatsphäre von Betroffenen muss so gering wie möglich gehalten werden. Es sollte daher bereits in der Behörde des Bundesbeauftragten sichergestellt werden, dass Akten über Betroffene der Stasi-Tätigkeit in eine erneute Überprüfung nicht wiederholt einbezogen werden, insbesondere dann nicht, wenn diese Unterlagen Daten aus der Intimsphäre enthalten.

Das StUG selbst sieht ein Mitteilungsverbot über eine inoffizielle Tätigkeit für das Ministerium für Staatssicherheit vor dem 31. Dezember 1975 vor (§ 19 Abs. 1 Satz 2 StUG). Der Rechtsgedanke, dass eine weit zurückliegende inoffizielle Tätigkeit für den Staatssicherheitsdienst nicht grundsätzlich die Eignung des Betreffenden für eine Tätig-

keit im öffentlichen Dienst in Frage stellt, sollte durch eine angemessene Dynamisierung des Mitteilungsverbotes über eine Mitarbeit, die länger als 20 Jahre zurückliegt, fortgeführt werden.

Eine schematische Auswertung von Überprüfungsergebnissen entspricht weder dem Zweck der Überprüfungen, noch berücksichtigt sie die Fehleranfälligkeit der Akten und das Recht der Betreffenden, sich zu Vorwürfen äußern zu können. Sie muss daher ausgeschlossen werden.

Die Verwendung der Stasi-Unterlagen ist auf den Zweck der Überprüfung beschränkt. Eine Zweckentfremdung von Überprüfungsergebnissen muss in jedem Fall ausgeschlossen werden. Insbesondere dürfen Informationen, die im Rahmen einer Überprüfung erlangt wurden, nicht zur öffentlichen Anprangerung, zur politischen Rechtfertigung, zur Titelaberkennung oder bei Beförderungsentscheidungen genutzt werden. Die Strafvorschrift des § 44 StUG sollte dahingehend erweitert werden, dass jedes unbefugte, zweckfremde Mitteilen von Informationen auch über eine inoffizielle Tätigkeit strafbar ist.

Rechte der Betroffenen

Die ursprüngliche Fassung des Stasi-Unterlagen-Gesetzes räumte Betroffenen und Dritten ein Antragsrecht auf Anonymisierung der sie betreffenden Daten ab dem 1. Januar 1997 ein. Der Gesetzgeber hat diesen Termin auf den 1. Januar 2003 verschoben. Den Betroffenen und Dritten sollte aber bereits jetzt zumindest ein Widerspruchsrecht gegen die Verabeitung ihrer personenbezogenen Unterlagen durch den Bundesbeauftragten für die Stasi-Unterlagen eingeräumt werden, wenn sie auf Grund ihrer besonderen Situation überwiegende schutzwürdige Gründe gegen diese Verarbeitung anführen können. Eine solche Regelung würde auch dem Rechtsgedanken des Art. 14 a) der Europäischen Datenschutzrichtlinie Rechnung tragen, die jedem ein Widerspruchsrecht gegen die prinzipiell rechtmäßige Verarbeitung seiner Daten aus überwiegenden, schutzwürdigen, sich aus seiner besonderen Situation ergebenden Gründen einräumt.

Weiterhin sollten im Zusammenhang mit der Weitergabe von personenbezogenen Daten für Zwecke der Forschung, der politischen Bildung und der Berichterstattung durch die Medien (§§ 32, 34 StUG) die Informationsrechte der betroffenen Personen gestärkt werden. Dabei kann es nicht darum gehen, den Amtsträgern bzw. Personen der Zeitgeschichte, Mitarbeitern und Begünstigten des Staatssicherheitsdienstes generell die Möglichkeit zu eröffnen, diese Weitergabe zu unterbinden. Sie sollten aber vorab bzw. zeitgleich zumindest über die Weitergabe informiert werden.

Schließlich sind Fälle bekannt geworden, in denen öffentliche Dienstherren ehemaligen Mitarbeitern des Ministeriums für Staatssicherheit, die bei ihnen beschäftigt waren, Einsicht in die sie betreffen-

den Bescheide des Bundesbeauftragten für die Stasi-Unterlagen unter Hinweis auf das Stasi-Unterlagen-Gesetz generell verweigert haben. Auch eine Abwägung der berechtigten Interessen der betroffenen Opfer und Dritter am Schutz ihrer personenbezogenen Daten mit dem rechtlichen Interesse ehemaliger Mitarbeiter der Staatssicherheit kann jedoch nicht dazu führen, dass einem ehemaligen Mitarbeiter des Staatssicherheitsdienstes die Möglichkeit der Rechtsverteidigung derart verkürzt wird.

Aufbewahrung der personenbezogenen Unterlagen

Die sichere, vor unbefugtem Zugang geschützte Aufbewahrung von personenbezogenen Unterlagen ist grundlegendes Anliegen des Datenschutzes.

Ergebnisse von Überprüfungen müssen gesondert von den allgemeinen Personalunterlagen aufbewahrt werden. Die Einsicht in diese Unterlagen ist auf einen begrenzten Personenkreis zu beschränken und zu protokollieren.

Darüber hinaus sind differenzierte Aufbewahrungsfristen festzulegen, die dem Grundsatz der Erforderlichkeit Rechnung tragen und sich am zeitlichen Rahmen der Überprüfung hinsichtlich des Mitteilungsverbotes über eine lang zurückliegende inoffizielle Tätigkeit für den Staatssicherheitssdienst (§ 19 StUG) und dem Ende des Überprüfungsprozesses im Jahre 2006 (§ 20 Abs. 3 StUG) orientieren.

Nach Ablauf dieser Frist müssen die Unterlagen unverzüglich gelöscht werden, soweit sie nicht auf Grund gesetzlicher Vorschriften Archiven angeboten und von diesen angenommen werden.

Es muss sichergestellt werden, dass personenbezogene Daten, die der Bundesbeauftragte für die Stasi-Unterlagen an andere Stellen herausgegeben hat, nach Erledigung der Aufgaben dieser Stellen an den Bundesbeauftragten zurückgegeben bzw. vernichtet werden, soweit nicht gesonderte Archivgesetzbestimmungen ein anderes regeln. Grundsätzlich muss verhindert werden, dass neben den Archiven des Bundesbeauftragten weitere Archive personenbezogene Unterlagen des Staatssicherheitsdienstes oder Kopien davon aufbewahren.

Anlage 3

Auszug aus dem Geschäftsverteilungplan des Berliner Beauftragten für Datenschutz und Akteineinsicht

Prof. Dr. Hansjürgen Garstka	**Berliner Datenschutzbeauftragter**
Cristina Vecchi	Sekretariat
	Zentraler Bereich
Prof. Dr. Hansjürgen Garstka	Bereichsleiter
	Zentrale Aufgaben
Birgit Saager	Arbeitsgebiete: Arbeit und Frauen, Arbeitnehmerdatenschutz
Anja-Maria Gardain	Arbeitsgebiete: Internationaler und europäischer Datenschutz, Verkehr, Justitiariat
Dipl. Informatiker Sven Mörs	Arbeitsgebiet: Telekommunikation und Medien
Dipl. Germanistin Laima Nicolaus	Sekretariat, Bibliothek, Rechtsprechungssammlung
	Allgemeine Verwaltung
Doris Werth	Büroorganisation, Haushaltsplanung und -bewirtschaftung
Alexandra Bertermann	Personalsachbearbeitung, Beschaffungswesen, Hausverwaltung
Monika Klößing	Sekretariat, Rechnungsstelle
	Bereich Recht
Claudia Schmid	Vertreterin des Datenschutzbeauftragten, Bereichsleiterin, Arbeitsgebiete: Datenschutzrecht, Nachrichtendienste, Verfassungsorgane, Presse- und Öffentlichkeitsarbeit, Pressesprecherin

Anlage 4

	Recht I
Dr. Ulrich von Petersdorff	Arbeitsgebiete: Gesundheit und Soziales, Kultur
Dipl. Volkswirt Dr. Rainer Metschke	Arbeitsgebiete: Schule, Wissenschaft, Forschung und Statistik
Daniel Holzapfel	Arbeitsgebiet: Wirtschaft
Kerstin Göhler	Sekretariat
	Recht II
Volker Brozio	Arbeitsgebiete: Bauen und Wohnen, Stadtentwicklung und Umweltschutz, Inneres (Ausländerangelegenheiten), Redaktion von Veröffentlichungen
Dagmar Hartge	Arbeitsgebiete: Finanzen, Justiz
Detlef Schmidt	Arbeitsgebiete: Bürgerberatung, Inneres, Bezirksämter
Sabine Krissel	Sekretariat
	Bereich Informatik
Dipl. Informatiker Hanns-Wilhelm Heibey	Vertreter des Datenschutzbeauftragten, Bereichsleiter, Grundsatzfragen des technischen Datenschutzes, Methoden der informationstechnischen Sicherheit, Arbeitsgebiete: Recht und Politik der Informationstechnik, Spezielle Anwendungen (Komplexe IT-Verfahren, Chipkarten)
Nicole Müller	Sekretariat, Führung der Dateienregister, Informationsmaterial
	Informatik I
Dipl. Physiker Joachim Laß	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Proprietäre Systeme, Sicherheit in Rechenzentren), nicht-automatisierte Datenverarbeitung

Jürgen Horn	Arbeitsgebiet: Organisation des Datenschutzes (Führung der Dateienregister, Betreuung der betrieblichen und behördlichen Datenschutzbeauftragten, Koordination von Beratung und Prüfung); Behördlicher DSB
Dipl. Informatiker (FH) Ralf Hauser	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Personalcomputer, PC-Netze)
	Informatik II
Dipl. Informatikerin Ursula Meyer zu Natrup	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Kommunikationssysteme), Spezielle Anwendungen (Bürokommunikation); Frauenvertrete-
rin	
Carsten Schmidt	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Offene Client-Server-Systeme)
Frank Holzkamp	Realisierung des Internetangebots
André Drescher	Systemverwaltung
Berliner Beauftragter für Datenschutz und Akteneinsicht	**Pallasstraße 25, 10781 Berlin, Telefon: (0 30) 78 76 88 44, Telefax: (0 30) 2 16 99 27, E-mail: mailbox@datenschutz-berlin.de, Internet: www.datenschutz-berlin.de**
Stand: Januar 2000	

Anlage 4

Abkürzungsverzeichnis

Nicht aufgenommen sind Abkürzungen, die nur in einem bestimmten Kapitel verwendet und dort erklärt werden, sowie allgemein bekannte Abkürzungen

Abghs.-Drs.	Abgeordnetenhaus-Drucksache
ABIEG	Amtsblatt der Europäischen Gemeinschaften
AO	Abgabenordnung
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BR-Drs.	Bundesrats-Drucksache
BSHG	Bundessozialhilfegesetz
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidungen
DNA	(deutsch: DNS) Desoxyribonu[se]kleinsäure
E-Mails	Electronic Mails
EDV	Elektronische Datenverarbeitung
EU	Europäische Union
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GGO I	Gemeinsame Geschäftsordnung für die Berliner Verwaltung I
GVBl.	Gesetz- und Verordnungsblatt
IFG	Informationsfreiheitsgesetz
ISDN	Integrated Services Digital Network
ISVB	Informationssystem Verbrechensbekämpfung
IT	Informationstechnik
luKDG	Informations- und Kommunikationsdienstegesetz
JB	Jahresbericht

Abkürzungsverzeichnis

LPD	Landespressedienst
MDK	Medizinischer Dienst der Krankenkassen
MiStra	Mitteilungen in Strafsachen
Mizi	Mitteilungen in Zivilsachen
NJW	„Neue Juristische Wochenschrift“
NStZ	Neue Steuerrecht-Zeitung
PIN	Persönliche Identifikationsnummer
SGB	Sozialgesetzbuch
SIM	Subscriber Identity Module
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
VwGO	Verwaltungsgerichtsordnung
WWW	World Wide Web

Stichwortverzeichnis

Stichwortverzeichnis

Stichwortverzeichnis

Stichwortverzeichnis

Stichwortverzeichnis