Tätigkeitsbericht

des Landesbeauftragten für den Datenschutz und

für das Recht auf Akteneinsicht

zum 31. Dezember 1999

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung jährlich einen Bericht über seine Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz, § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 3. März 1999 vorgelegten Tätigkeitsbericht 1998 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 1999 ab.

Der vorliegende Bericht enthält erstmals im Anschluss an das Inhaltsverzeichnis ein Behördenverzeichnis, das es den Bürgerinnen und Bürgern, aber auch der Landesregierung ermöglichen soll, Ergebnisse unserer Tätigkeit auch in ressortübergreifenden Kapiteln leichter zu finden.

Inhaltsverzeichnis Seite

Teil B

Akteneinsicht und Informationszugang

Teil C

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Anlagen

Dokumente zum Datenschutz 1999

A. Beschlüsse und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

- Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften
- "Täter-Opfer-Ausgleich und Datenschutz"
- Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung
- Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union
- Patientenschutz durch Pseudonymisierung
- DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen
- Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

B. Datenschutzbeauftragte fordern Trendwende in der Telekommunikationspolitik: Weg vom Anspruch auf lückenlose Überwachung hin zu einem effektiven Schutz des Fernmeldegeheimnisses

- Für eine Sicherung der freien Telekommunikation in unserer Gesellschaft

C. Beschlüsse der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation

- Gemeinsamer Standpunkt zu Datenschutz bei Gebäude-Bilddatenbanken
- Gemeinsamer Standpunkt zu intelligenten Software-Agenten
- Gemeinsamer Standpunkt zur Sprechererkennung und Stimmerkennungstechnologien in der Telekommunikation

D. Arbeitspapier der Datenschutzbeauftragten der Europäischen Union (Gruppe nach Art. 29 der Datenschutzrichtlinie der EU)

- Über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware

Behördenverzeichnis

	Gliederungspunkt
Bauverwaltung	A 4.5.1 B 3.4
Einwohnermeldeamt	A 4.3.1 A 4.3.2 A 8.2.1
Finanzamt	A 3.3.1 A 3.3.2 A 12.1
Führerscheinstelle	A 11.1
Gesundheitsamt	A 6.4 A 8.3.2
Investitionsbank des Landes Brandenburg	A 9.1
Jugendamt	A 6.5
Katasteramt	A 11.2
Krankenhaus	A 8.2.2 A 8.3.1
Landesamt für Datenverarbeitung und Statistik	A 2.1.4 A 2.1.6 A 2.1.7 A 3.3.4 A 4.5.1 A 4.5.2
Landesamt zur Regelung offener Vermögensfragen	A 3.3.3
Landesbauamt	A 3.3.1

	A 3.3.3
Landesklinik	A 8.3.1
Landeskriminalamt	A 4.1.4
Landesrechnungshof	A 4.4.2
Ministerium der Finanzen	A 3.3.1 A 3.3.2 A 3.3.3 B 2.2
Ministerium der Justiz und für Europaangelegenheiten	A 4.1.3 A 4.4.1 A 5.7 B 2.2 B 3.5
Ministerium des Innern	A 1.1 A 2.1.1 A 4.1.1 A 4.1.4 A 4.5.1 A 4.5.2 A 6.1.2 A 8.1 B 2.1 B 2.2 B 3.5
Ministerium für Arbeit, Soziales, Gesundheit und Frauen	A 8.1 A 8.2.1 A 8.2.2 A 8.3.1
Ministerium für Bildung, Jugend und Sport	A 2.1.2 A 6.1.1

	A 6.1.2 A 6.5 A 6.6 A 6.7
Ministerium für Ernährung, Landwirtschaft und Forsten	A 10.2 B 2.2
Ministerium für Stadtentwicklung, Wohnen und Verkehr	A 3.3.1 A 11.2 A 11.3
Ministerium für Wirtschaft	A 9.1.1 A 9.1.2
Ministerium für Wissenschaft, Forschung und Kultur	A 7.1
Oberfinanzdirektion	A 2.1.1 A 3.3.1 A 4.4.4
Oberlandesgericht Brandenburg	A 5.5 A 5.6
Oberverwaltungsgericht	B 3.5
Polizei	A 2.1.1 A 4.1.1 A 4.1.4 A 5.2 A 8.2.1 A 11.1
Sozialamt	A 3.4.3 A 8.2.1
Sozialgericht	A 8.2.3
Staatliches Schulamt	A 2.1.2

Staatsanwaltschaft	A 5.2 A 8.2.1 A 9.1 A 11.1 B 3.5
Staatskanzlei	A 2.1.3 A 3.4.3 C 3
Untere Bauaufsichtsbehörde	A 11.3
Verfassungsschutz	A 4.1.4 A 4.2 A 9.1
Zentrale Bezügestelle des Landes Brandenburg	A 4.4.3 A 12.2

Einleitung

In letzter Zeit wird zunehmend das "Ende der Privatheit" heraufbeschworen. Der Top-Manager eines führenden US-Computerherstellers drückt das so aus: "Sie haben keine Privatsphäre mehr. Finden Sie sich damit ab." Damit bezieht er sich in erster Linie auf die vielfältigen Spuren, die die meisten Nutzerinnen und Nutzer im Internet hinterlassen und die zur minutiösen Registrierung Einzelner und deren Nutzungsgewohnheiten für kommerzielle Zwecke führen. Ab März 2000 strahlt - 50 Jahre nach dem Tode George Orwells - in Deutschland ein privater Fernsehsender ausgerechnet unter dem Titel "Big Brother" eine Show aus, in der sich zehn Menschen 100 Tage lang von Kameras und Mikrophonen bei jeder Bewegung und jeder Äußerung beobachten lassen[1]. Nachdenklich stimmt nicht nur, dass die Veranstalter dieser Sendung sich vor Interessenten für die aktive Teilnahme kaum retten können, sondern auch, dass diese schon in den Niederlanden sehr erfolgreiche Sendung auch hier offenbar mit hohen Einschaltquoten rechnen kann. Ob derartige Veranstaltungen, bei denen Menschen bis in die letzten Momente ihrer Privatheit gezeigt werden, mit den Bestimmungen des Rundfunkrechts zum "Reality-TV" zu vereinbaren sind, müssen die entsprechenden Aufsichtsbehörden entscheiden.

Es wäre aber ein Fehlschluss zu glauben, der hierbei sichtbar werdende Exhibitionismus sei ein Beleg dafür, dass der Schutz der Privatsphäre und der persönlichen Daten am Ende des 20. Jahrhunderts verzichtbar ist. Unsere Erfahrungen zeigen eher das Gegenteil: Immer wieder wenden sich Bürgerinnen und Bürger an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, um den Umgang staatlicher Stellen mit ihren persönlichen Daten, aber auch mit anderen Informationen überprüfen zu lassen. Das ist ihr gutes Recht, denn kein Mensch braucht es nach unserer Verfassung hinzunehmen, dass öffentliche Stellen über die Preisgabe seiner persönlichen Daten ohne Rechtsgrundlage und gegen seinen Willen befinden oder ihm grundlos den Zugang zu amtlichen Unterlagen verweigern. Dabei hat der unabhängige Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, wie das Verfassungsgericht des Landes Brandenburg hervorgehoben hat[2], im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen zum Grundrechtsschutz beizutragen. Dass dies angesichts der gerade in Brandenburg besonders deutlichen Überlastung der Verwaltungsgerichte immer wichtiger wird, hat sich im Berichtszeitraum mehrfach erwiesen[3]. Der Landesbeauftragte kann die Kontrolle des Verwaltungshandelns durch Gerichte allerdings nicht ersetzen, sondern nur im Vorfeld gerichtlicher Auseinandersetzungen zur Konfliktlösung und damit auch zur Entlastung der Gerichte beitragen.

Datenschutz und Informationszugang werden auch durch die weitere Entwicklung des Internets an Bedeutung

---

1 Die "Märkische Allgemeine Zeitung" vom 21.1.2000 machte auf diesen zeitlichen Zusammenhang aufmerksam.

2 Urteil vom 30.6.1999 - VfGBbg 3/98 -, S. 45

3 s. unter A 4.2 und B 3.5

zunehmen. Im November 1997 lag in Brandenburg der Anteil derer, die einen Internet-Anschluss hatten, bei nur vier Prozent. Nur 19 Prozent gaben an, wahrscheinlich innerhalb der nächsten zwei Jahre das Medium "Internet" nutzen zu wollen. Für die weitere Ausbreitung dieses Mediums wird viel davon abhängen, dass das Vertrauen in die sichere und verlässliche Kommunikation gestärkt und die Nutzerfreundlichkeit deutlich erhöht wird. Hierfür hat die Bundesregierung in den kommenden fünf Jahren erhebliche Investitionen vorgesehen. Es gilt darüber hinaus, für Informationsgerechtigkeit zu sorgen, also eine Teilung der Gesellschaft in zwei Gruppen zu vermeiden, von denen sich die "Informationsbesitzer" Zugang zu Informationen leisten können, während die "Habenichtse" dies nicht können. Mit dieser Thematik setzt sich die Landesregierung im Rahmen der Brandenburgischen Informationsstrategie 2006 (BIS2006) mit ihren verschiedenen Arbeitsgruppen auseinander, an denen wir uns auch im vergangenen Jahr beteiligt haben.

Ob es gelingt, die Architektur des Internets und anderer offener Kommunikationsnetze datenschutzgerechter zu gestalten, ist gegenwärtig völlig offen. Allein die Tatsache jedoch, dass dieser Versuch auch international unternommen wird, zeigt, dass der Datenschutz gerade im Zeitalter des Internets immer wichtiger wird. Wer Hard- und Software herstellt, muss sich zunehmend mit den berechtigten Forderungen nach der Entwicklung datenschutzfreundlicher Produkte auseinander setzen und stößt auf den Widerstand der Verbraucherinnen und Verbraucher, wenn er sich darüber hinwegsetzen will. Beispielsweise scheiterten Hersteller von Software und Mikroprozessoren bei dem Versuch, ihre Produkte verdeckt zu kennzeichnen, um so das Nutzungsverhalten im Internet heimlich registrieren zu können. Die Datenschutzbeauftragten des Bundes und der Länder haben die Notwendigkeit der Entwicklung und des Einsatzes von transparenter Hard- und Software betont[4]. Gerade weil die Bürgerinnen und Bürger in Zukunft solche Produkte zunehmend auch dazu nutzen werden, um mit der Verwaltung in Verbindung zu treten, ist es von entscheidender Bedeutung, dass die Technik es ihnen ermöglicht, über die Preisgabe und Verwendung ihrer personenbezogenen Daten selbst zu entscheiden.

Es hat im vergangenen Jahr für den Datenschutz aber auch Rückschläge gegeben. Dazu zählte vor allem das teilweise Scheitern des Gesetzentwurfes der Bundesregierung zur Gesundheitsreform 2000. Er sah zunächst vor, dass die Krankenkassen künftig von den Ärztinnen und Ärzten, Krankenhäusern oder Apotheken die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten sollten. Dieses neue Modell hätte eine zentrale Forderung der Datenschutzbeauftragten aufgenommen, für die Verarbeitung von Patientendaten nur solche Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des "gläsernen Patienten" verhindern[5]. Es bleibt zu hoffen, dass dieser Teil der Gesetzesreform wieder aufgegriffen und verabschiedet wird, weil damit ein Durchbruch zur datenschutzfreundlichen Gestaltung des Abrechnungsverfahrens

[4] Entschließung vom 26. 3. 1999, Dokumente zum Datenschutz, Teil A I

[5] s. die beiden Entschließungen der Datenschutzkonferenz vom August und Oktober 1999, Dokumente zum Datenschutz 1999, Teil A II und III

im Gesundheitswesen erzielt werden könnte.

Kontrovers diskutiert wird in letzter Zeit die Frage, wie mit Stasi-Unterlagen zur Überprüfung von Abgeordneten und öffentlichen Bediensteten verfahren werden sollte. Diese Diskussion greift sicherlich zu kurz, soweit für einen generellen "Schlussstrich" zehn Jahre nach der Wende im Osten Deutschlands plädiert wird. Allerdings werfen der Umfang der Überprüfung, der betroffene Personenkreis, die weitere Nutzung und Aufbewahrung von Stasi-Unterlagen sowie die Rechte der Betroffenen Fragen auf, die einer Antwort bedürfen. Hierzu haben wir mit den Landesbeauftragten in Mecklenburg-Vorpommern und Berlin Vorschläge formuliert, die wir zur Diskussion stellen[6]. Auch die im Land Brandenburg von der Landesregierung 1995 beschlossenen Grundsätze für die Überprüfung von Landesbediensteten haben bisher nicht dazu geführt, dass sich hier eine einheitliche Praxis herausgebildet hat.

Der Landesbeauftragte für den Datenschutz hat zugleich die Aufgabe, zur Wahrung des Grundrechts auf Akteneinsicht und Informationszugang beizutragen. Das Brandenburgische Akteneinsichts- und Informationszugangsgesetz kann als spätes Ergebnis der Bürgerrechtsbewegung in der ehemaligen DDR angesehen werden, das inzwischen auch Wirkungen außerhalb Brandenburgs zeigt. Es ist besonders erfreulich, dass die Länder Berlin und Schleswig-Holstein inzwischen ihren Bürgerinnen und Bürgern durch die Verabschiedung von Informationsfreiheitsgesetzen ebenfalls ein allgemeines Akteneinsichtsrecht eröffnet haben. Das Beispiel Brandenburgs macht Schule und es ist zu hoffen, dass weitere Länder wie auch der Bund diesem Beispiel folgen werden.

Bürgerinnen und Bürger in Brandenburg wenden sich zunehmend an uns mit der Bitte um Beratung und Unterstützung. Wenn Einzelne oder Bürgerinitiativen Akteneinsicht verlangen, so muss dies nicht zur Aufdeckung großer Skandale führen; vielmehr ist es eine unspektakuläre, aber wichtige Voraussetzung für bürgerschaftliches Engagement in der Gemeinde und vor Ort. Demokratie als Staatsform ist für viele ein zu abstrakter Begriff, um sich damit zu identifizieren. Offenheit und Transparenz der täglichen Verwaltungsentscheidungen zur Planung von Straßen, zum Ausbau von Spazierwegen oder zum Brandschutz in Schulen hingegen sind kleine, aber wichtige Voraussetzungen der Demokratie, die in Brandenburg von allen eingefordert werden können.

Dass es dabei zu Schwierigkeiten und Enttäuschungen auf Seiten der Bürgerinnen und Bürger kommt, liegt zum einen an einer in der Verwaltung noch weit verbreiteten Mentalität des "Da kann ja jeder kommen!". Zum anderen verhindert aber auch die restriktive Fassung des Gesetzes den Informationszugang selbst in solchen Fällen, in denen die Offenlegung der Unterlagen von der Sache her selbst der Verwaltung gerechtfertigt erscheint.

---

[6] Anlage 1

Festzuhalten bleibt aber bei aller Kritik im Detail, dass Brandenburg als erstes Bundesland einen wichtigen Schritt hin zu mehr Verwaltungstransparenz unternommen und einzelnen Bürgerinnen, Bürgern und Bürgerinitiativen ein einklagbares Recht auf Zugang zu den Unterlagen der öffentlichen Verwaltung eingeräumt hat. Die Erfahrungen mit dem Informationsfreiheitsgesetz in den USA zeigen, dass dies möglicherweise der erste Schritt zur Verwirklichung des Grundrechts auf Informationszugang ist. Schon jetzt wird deutlich, dass die Entscheidung des Gesetzgebers für mehr Verwaltungstransparenz in Brandenburg zu einem wichtigen Bestandteil einer bürgerfreundlichen Verwaltungsreform werden kann.

Teil A

Datenschutz

1 Entwicklung des Datenschutzrechts

1.1 Gerät die Modernisierung des Bundesdatenschutzgesetzes ins Stocken?

Obwohl die von der Europäischen Datenschutzrichtlinie vorgegebene Anpassungsfrist bereits seit mehr als einem Jahr verstrichen ist, hat die Bundesregierung im Berichtszeitraum entgegen ihrer mehrfachen Ankündigung noch immer nicht über den Entwurf für ein novelliertes Bundesdatenschutzgesetz beschlossen. Damit wird ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland vor dem Europäischen Gerichtshof immer wahrscheinlicher. Ursprünglich war ein Beschluss des Bundeskabinetts bereits für Oktober 1999 vorgesehen, er wurde allerdings bisher immer wieder verschoben. Die notwendige Anpassung an die EG-Datenschutzrichtlinie auf Bundesebene wird deshalb auch bis zur Sommerpause 2000 nicht vollzogen werden.

Wir haben zum Entwurf des Bundesinnenministeriums bereits im August 1999 Stellung genommen, da ursprünglich mit einer Befassung des Bundesrates noch vor Jahresende gerechnet wurde. Der Gesetzentwurf, der zwischenzeitlich erneut überarbeitet worden ist, enthält zwar gewisse Ansätze für eine Modernisierung des Datenschutzrechts in Deutschland; so haben der auch im Brandenburgischen Datenschutzgesetz verankerte Grundsatz der Datensparsamkeit sowie Regelungen zum Datenschutzaudit, zu Chipkarten und zur Videoüberwachung Eingang in den Entwurf gefunden. Allerdings lässt dieser die Vorschläge der Datenschutzbeauftragten des Bundes und der Länder für eine grundlegende Weiterentwicklung in diesem Bereich[7] weitgehend unberücksichtigt.

Außerdem ist kritisch anzumerken, dass der Gesetzentwurf schon für Juristinnen und Juristen, erst recht aber für die betroffenen Laien schwer lesbar und in Teilen geradezu abschreckend unverständlich formuliert ist. Wer den Entwurf liest, muss den Eindruck gewinnen, beim Datenschutzrecht handele es sich um eine Art "Rokoko des Rechtsstaats"; dabei gerät aus dem Blick, dass hier das Grundrecht auf Datenschutz für den Bereich der Bundesverwaltung und den immer wichtiger werdenden Bereich der privaten Wirtschaft präzisiert wird.

Im Einzelnen haben wir kritisiert, dass sich der Gesetzentwurf nach wie vor am Dateibegriff orientiert und damit die Datenverarbeitung in Akten in der Privatwirtschaft ausklammert und damit privilegiert. Eine derartige Privilegierung ist aber nicht zu rechtfertigen. Es ist niemandem verständlich zu machen, wieso das Datenschutzniveau unterschiedlich hoch sein soll, je nachdem, ob Daten in Dateien oder in Akten gespeichert sind. In vielen Punkten

[7] s. Dokumente zum Datenschutz 1999, Teil A I

hat das Bundesinnenministerium es versäumt, sich an modernen Regelungen z. B. des neuen Brandenburgischen Datenschutzgesetzes zu orientieren. Teilweise würde die Verabschiedung des Entwurfs auf Bundesebene sogar zu einer Verschlechterung des Datenschutzstandards führen.

Auch ist die bisher vorgesehene Regelung zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nicht geeignet, dem Problem der immer stärkeren Verbreitung von kommerziellen Bilddatenbanken, etwa von Gebäuden, adäquat zu begegnen. Zu diesem Problem hat die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation im vergangenen Jahr auf Initiative des Brandenburgischen Landesbeauftragten einen gemeinsamen Standpunkt erarbeitet, der das Widerspruchsrecht der Gebäudeeigentümerinnen und -eigentümer gegen die systematische Erfassung von Gebäuden in derartigen Datenbanken für kommerzielle Zwecke hervorhebt[8].

Wie bisher sollen personenbezogene Daten aus Abhörmaßnahmen des Verfassungsschutzes und der Nachrichtendienste, die der Kontrolle durch die sog. G 10-Kommission unterliegen, pauschal der Kontrolle durch die Datenschutzbeauftragten entzogen bleiben. Nur ausnahmsweise können diese von der G 10-Kommission ersucht werden, die Einhaltung der Datenschutzvorschriften zu kontrollieren und ihr darüber zu berichten. Es bestehen erhebliche Zweifel, ob dieses Kontrollmodell für Eingriffe in das Telekommunikationsgeheimnis dem Grundsatzurteil des Bundesverfassungsgerichts vom 14. Juli 1999 zur verdachtslosen Rasterfahndung des Bundesnachrichtendienstes[9] entspricht. Das Gericht hat in dieser Entscheidung zum einen die grundlegende Bedeutung des Telekommunikationsgeheimnisses in der Informationsgesellschaft hervorgehoben[10] und zum anderen Kontrolldefizite beim Umgang mit Daten festgestellt, die durch Abhörmaßnahmen erhoben wurden.

Diese Kontrolldefizite können nicht allein durch eine Erweiterung der Befugnisse der G 10-Kommission behoben werden, die gegenwärtig auf Bundesebene diskutiert wird. Vielmehr müssen auch die Datenschutzbeauftragten eindeutige Kontrollbefugnisse zumindest in dem Bereich erhalten, in dem personenbezogene Daten aus Abhörmaßnahmen weiter verwendet werden. Hier haben die G 10-Kommissionen bisher weder auf Bundes- noch auf Landesebene Kontrollzuständigkeiten. Sie entscheiden nur über das "Ob" der Abhörmaßnahme. Insbesondere für den Bereich der Landesverwaltung hat das Bundesverfassungsgericht ausdrücklich angemahnt, dass eine ausreichende Kontrolle der Weiterverwendung gewährleistet sein muss, soweit Daten aus Abhörmaßnahmen, z. B. des Bundesnachrichtendienstes, an Landesbehörden übermittelt werden[11]. Diese Daten unterliegen nicht der Kontrolle durch die G 10-Kommission des Landes. Insofern sollte der Landesbeauftragte eine Kontrollbefugnis

8 s. Dokumente zum Datenschutz 1999, Teil C

9 1 BvR 226/94 u. a., EuGRZ 1999, S. 389 ff.

10 dazu unten 3.1

11 BVerfG a. a. O. S. 415

erhalten, die im Entwurf des Bundesinnenministeriums für ein neues Bundesdatenschutzgesetz bisher ausgeschlossen ist.

Schließlich sollte auch das Bundesdatenschutzgesetz die Zweckentfremdung von Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung nur noch mit Einwilligung der Betroffenen zulassen. Die bisherige Privilegierung des Adresshandels und der Markt- und Meinungsforschung ist nicht länger gerechtfertigt, zumal sowohl im Telekommunikations- wie auch im Teledienstерecht die Nutzung von Bestandsdaten entsprechend restriktiv geregelt ist.

Das Bundesinnenministerium will außerdem einen Auskunftsanspruch der Betroffenen über die zu ihrer Person gespeicherten Daten schon dann ausschließen, wenn dem ein überwiegendes Interesse an der Wahrung von Betriebs- und Geschäftsgeheimnissen entgegensteht. Diese Einschränkung ist nicht gerechtfertigt und widerspricht neben deutschem Verfassungsrecht auch der EG-Datenschutzrichtlinie. Wirtschaftliche Interessen der verantwortlichen Stellen können den Auskunftsanspruch der Betroffenen (die "Magna Charta" des Datenschutzes) nicht beschränken.

Völlig inakzeptabel sind die im Entwurf vorgesehenen langen Übergangszeiträume von drei bis fünf Jahren.

Durch entsprechende Konkurrenzklauseln will das Bundesinnenministerium schließlich verhindern, dass der Datenschutz auch im Bereich der Sicherheitsbehörden modernisiert wird. Selbst wenn hier kein unmittelbarer Umsetzungsbedarf aufgrund der EG-Richtlinie besteht, hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stets gegen die Einführung unterschiedlicher Datenschutzstandards im Anwendungsbereich der Richtlinie einerseits und im Sicherheitsbereich andererseits gewandt.

Das Ministerium des Innern hat einen Teil unserer Kritik am Gesetzentwurf des Bundesinnenministeriums übernommen.

Die Koalitionsfraktionen im Bundestag haben sich dem Vernehmen nach darauf verständigt, noch vor der Verabschiedung des novellierten Bundesdatenschutzgesetzes in einer sog. "zweiten Welle" mit Vorarbeiten für eine grundlegende Modernisierung des Datenschutzrechts in Deutschland zu beginnen. Hierzu soll eine Arbeitsgruppe von Sachverständigen eingesetzt werden. Gegenwärtig sind aber angesichts des langsamen Fortschritts der noch nicht einmal vom Bundeskabinett beschlossenen BDSG-Novelle Zweifel angebracht, ob die grundlegende Reform des Datenschutzrechts noch in dieser Legislaturperiode gelingen kann. Dass eine solche grundlegende Reform überfällig ist, wird inzwischen von allen Seiten anerkannt. Sie darf aber nicht dazu genutzt werden, den Datenschutzstandard generell gegenüber dem bisher Erreichten abzusenken.

Zu einer Verzögerung der Arbeiten am Entwurf für ein neues Bundesdatenschutzgesetz hat auch die öffentliche Diskussion um das sog. Medienprivileg beigetragen. Der Entwurf des Bundesinnenministeriums sah zunächst vor, dass auch in Presseunternehmen interne betriebliche Datenschutzbeauftragte bestellt werden sollten und außerdem Personen, die durch eine Berichterstattung in ihrem Persönlichkeitsrecht beeinträchtigt werden, Auskunft über die der Berichterstattung zu Grunde liegenden, zu ihrer Person gespeicherten Daten verlangen können. Dabei sollte das Presseunternehmen nicht verpflichtet sein, Auskunft über Gewährspersonen und andere Quellen zu geben. Der Deutsche Presserat und mehrere Verbände der Zeitungsverleger haben die vorgesehenen Regelungen in die Nähe einer verfassungswidrigen Zensur gerückt. Diese Kritik ist überzogen und beruht teilweise auf mangelnder Sachkenntnis.

Journalistinnen und Journalisten müssen ungehindert ihren verfassungsrechtlich geschützten Recherchetätigkeiten nachgehen können, ohne Auskunft über ihre Informationsquellen geben zu müssen. Zugleich muss der Datenschutz von Bürgerinnen und Bürgern entsprechend der Europäischen Datenschutzrichtlinie auch gegenüber Presseunternehmen verbessert werden. Gerade der Anspruch der Betroffenen über die einer Berichterstattung zu Grunde liegenden Tatsachen bringt das Grundrecht auf Datenschutz auch im sensiblen Bereich der Presse angemessen zur Geltung. Da solche Ansprüche erst nach der Veröffentlichung geltend gemacht werden können, wird die Freiheit der Berichterstattung in keiner Weise beeinträchtigt. Für die meisten Rundfunkveranstalter und die Anbieter von Mediendiensten gilt dieser Auskunftsanspruch schon seit geraumer Zeit. Die Presse nimmt insoweit keine Sonderstellung ein. Auch der befürchteten Ausforschung des Informationsbestandes durch interessierte Personen kann durch entsprechende Regelungen, die es im Rundfunkrecht bereits gibt, begegnet werden. Dennoch hat die Kritik der Presse am Entwurf des Bundesinnenministeriums offenbar dazu geführt, dass die ursprünglich vorgesehenen geringfügigen Verbesserungen des Datenschutzstandards in diesem Bereich wieder zu Gunsten einer bloßen Selbstregulierung rückgängig gemacht worden sind.

1.2 Datenschutz und Informationszugang als europäische Grundrechte

Während die Brandenburgische Landesverfassung sowohl ein Grundrecht auf Datenschutz (Artikel 11) als auch auf Informationszugang und Akteneinsicht (Artikel 21 Abs. 3 und 4) enthält, fehlen vergleichbare ausdrückliche Verfassungsgarantien bisher im Grundgesetz. Um so bedeutsamer ist es, dass der Europäische Rat in Köln im Juni 1999 die Einsetzung eines Gremiums beschlossen hat, das eine Charta der Grundrechte der Europäischen Union erarbeiten soll. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dies in einer Entschließung[12] ausdrücklich begrüßt und sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union eingesetzt. Dies würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung tragen.

Darüber hinaus ist anzustreben, dass in einem zukünftigen europäischen Grundrechtskatalog auch das Grundrecht auf Informationszugang entsprechend dem Beispiel der Brandenburgischen Landesverfassung aufgenommen wird. Erst durch die Verknüpfung von informationeller Selbstbestimmung und informationeller Teilhabe und Mitbestimmung wird eine entscheidende Voraussetzung für die Entstehung einer europäischen Informationsgesellschaft der Bürgerinnen und Bürger geschaffen.

2 Technisch-organisatorische Entwicklungen

2.1 Das Landesverwaltungsnetz

2.1.1 Sicherheitskonzept - Oberfinanzdirektion bleibt in der Pflicht

In vorangegangenen Tätigkeitsberichten[13] sind wir bereits auf die Notwendigkeit der frühzeitigen Erstellung von Sicherheitskonzepten eingegangen. Positiv ist dabei hervorzuheben, dass vom Ministerium des Innern nun endlich das Sicherheitskonzept für das Kernnetz des Landesverwaltungsnetzes und das Fachnetz der Polizei fertiggestellt wurde. Dagegen ist nicht nachvollziehbar, dass die Oberfinanzdirektion als Betreiberin bisher immer noch kein Sicherheitskonzept für das Fachnetz der Finanzverwaltung erstellt hat. Bereits im April 1998 forderten wir die Betreiberin schriftlich auf, uns das ausstehende Sicherheitskonzept gem. § 26 Abs. 1 Nr. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) zur Verfügung zu stellen.

---

[12] s. Dokumente zum Datenschutz 1999, Teil A III

[13] s. 6. Tätigkeitsbericht unter 1.4.1 und Tätigkeitsbericht 1998 unter 2.1.1

Die Sicherheit im Kernnetz und in den Fachnetzen bleibt lückenhaft, solange die Oberfinanzdirektion kein eigenes Sicherheitskonzept vorlegt. Die Landesregierung sollte diese offene Flanke des Landesverwaltungsnetzes so bald wie möglich schließen.

2.1.2 Anschluss der staatlichen Schulämter an das Landesverwaltungsnetz

Seit einiger Zeit besteht beim Ministerium für Bildung, Jugend und Sport der Wunsch, die staatlichen Schulämter an das Landesverwaltungsnetz anzuschließen. Die staatlichen Schulämter betreiben ihrerseits das Personalinformationssystem APSIS (Automatisierte Personalverwaltung und Stellenbewirtschaftung im Schulamt), mit dem die personenbezogenen Daten der Lehrerinnen und Lehrer verarbeitet werden.

Wir hatten bereits in unserem 6. Tätigkeitsbericht 1997[14] hierüber berichtet und festgestellt, dass die APSIS-Daten nur schwach verschlüsselt sind und das System deshalb lediglich als kleines lokales, physikalisch eigenständiges Netz mit eigenem Server ohne Anschluss an andere lokale oder weite Netze betrieben werden darf.

Das Personalinformationssystem der Landesverwaltung (PERIS) verfügt dagegen über eine starke Verschlüsselung. Es kann deshalb bei entsprechender Konfigurierung auch in großen lokalen Netzen oder im Landesverwaltungsnetz betrieben werden.

Da nun einerseits frühestens Anfang 2001 eine starke Verschlüsselung für APSIS zur Verfügung stehen wird und andererseits der Anschluss an das Landesverwaltungsnetz möglichst bald verwirklicht werden soll, kann als Übergangslösung nur der Einsatz von zusätzlichen Firewalls vom Typ des Application Level Gateway mit zwei Netzschnittstellen in Frage kommen, um unzulässige Durchgriffe auf die Beschäftigtendaten zu verhindern. Diese Firewalls werden dann entweder zur Abschottung der APSIS-Netze gegenüber den Kreisverwaltungsnetzen oder gegenüber dem Landesverwaltungsnetz eingesetzt.

Unsere Vorschläge für eine solche Übergangslösung sind allerdings weder vom Ministerium noch von den Kreisverwaltungen aufgegriffen worden. Wir weisen ausdrücklich darauf hin, dass sich die technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit gemäß Brandenburgischem Datenschutzgesetz am jeweiligen Stand der Technik zu orientieren haben, d. h. - wie das Beispiel PERIS zeigt - es müssen starke Verschlüsselungsverfahren eingesetzt werden. Es ist darüber hinaus nicht hinzunehmen, dass die

[14] s. unter 13.2.1, S. 166 f.

Daten der Lehrerinnen und Lehrer über einen längeren Zeitraum erheblich weniger gut geschützt sein sollen als die Daten der übrigen Beschäftigten der Landesverwaltung.

Der beste Schutz für Beschäftigtendaten vor unberechtigtem Zugriff aus anderen Netzen ist der Einsatz von starker Verschlüsselung in Kombination mit gut konfigurierten Firewalls.

2.1.3 Kontrolle des Datennetzes der Staatskanzlei

Die Kontrolle des Datenetzes der Staatskanzlei ergab Mängel bei der Umsetzung technisch-organisatorischer Maßnahmen. So wurde u. a. festgestellt, dass das lokale Netz (LAN) unzureichend vom Landesverwaltungsnetz abgeschottet war. Der zentrale Router ließ es zeitweise zu, dass man vom Landesverwaltungsnetz aus nahezu mühelos auf das LAN der Landesbehörde zugreifen konnte. Hinzu kam, dass für einen Teil der aktiven Netzkomponenten (Switches) keine Passwörter vergeben waren. Zum Zeitpunkt der Kontrolle hätte ein potentieller Angreifer vom Landesverwaltungsnetz aus eine Reihe von Netzsegmenten dieser obersten Landesbehörde stilllegen können, sodass die Arbeitsfähigkeit ganzer Abteilungen beeinträchtigt gewesen wäre.

Wir haben die Staatskanzlei aufgefordert, das lokale Netz mit einer Firewall abzuschotten und die aktiven Netzkomponenten (Router, Switches) restriktiv zu konfigurieren. Die Staatskanzlei hat zugesagt, die festgestellten Mängel alsbald zu beheben. Das ist im Übrigen auch unabhängig von den datenschutzrechtlichen Anforderungen notwendig, um die Funktionssicherheit und Verfügbarkeit des Datennetzes sicherzustellen.

Werden personenbezogene Daten in einem lokalen Netz verarbeitet, welches am Landesverwaltungsnetz oder an einem anderen Weitverkehrsnetz angeschlossen ist, so muss das lokale Netz durch ein Firewallsystem abgeschottet werden. Welche Firewall-Technologie (Packet Filter, Application Level Gateway u. a.) zum Einsatz kommt, richtet sich nach der Sensibilität der im LAN verarbeiteten personenbezogenen Daten.

2.1.4 IT-Sicherheitsreport auf dem WWW-Server „Brandenburg Intern“

Es ist relativ selten, dass eine Software absolut fehlerfrei arbeitet. Daraus entstehen Sicherheitslücken, die aus Sicht der Datensicherheit und des Datenschutzes verheerende Folgen haben können. Die auch nicht seltenen Konfigurationsfehler tragen das Ihre zur Entstehung von Sicherheitslücken bei. ADV-Verantwortliche haben daher

die Pflicht, sich über bekannt gewordene Sicherheitslücken regelmäßig zu informieren. Die meisten Hersteller bieten entsprechende Informationen im Internet an.

Um besonders sicherheitsrelevante Informationen schnell verfügbar zu machen, haben wir als Dienstleistung für die Behörden in Brandenburg gemeinsam mit dem Landesamt für Datenverarbeitung und Statistik einen IT-Sicherheitsreport im Intranet des Landes auf dem WWW-Server „Brandenburg Intern“[15] eingerichtet mit Hinweisen auf aktuelle Sicherheitsprobleme in IT-Systemen. Wir würden es begrüßen, wenn sich auch andere öffentliche Stellen an dem IT-Sicherheitsreport beteiligten.

Gemeinsam mit dem Landesamt für Datenverarbeitung und Statistik stellt unsere Behörde auf dem WWW-Server „Brandenburg Intern“ Hinweise zu aktuellen Sicherheitsproblemen zur Verfügung.

2.1.5 Protokollierung von Nutzeraktivitäten auf WWW-Servern

Bereits in vorangegangenen Tätigkeitsberichten[16] haben wir auf die Problematik der Protokollierung von Nutzeraktivitäten auf WWW-Servern hingewiesen. Das Problem besteht darin, dass in den Protokolldateien der Server keine IP-Adressen gespeichert werden dürfen, da nicht auszuschließen ist, dass eine IP-Adresse einer bestimmten Person zugeordnet werden kann, und die Speicherung von personenbezogenen Protokolldateien auf WWW-Servern aus datenschutzrechtlicher Sicht unzulässig ist.

Im letzten Berichtszeitraum haben wir fünf WWW-Server überprüft. Erfreulicherweise konnten wir feststellen, dass bei allen WWW-Servern die Protokollierung entweder ganz abgeschaltet war oder in anonymisierter Form erfolgte. Die Vorgaben des Multimedia-Rechts werden offenbar von den öffentlichen Stellen Brandenburgs stärker als in der Vergangenheit beachtet.

Nutzerzugriffe auf WWW-Server dürfen nur in anonymisierter Form protokolliert werden. Kontrollen im Berichtszeitraum ergaben diesbezüglich keine Mängel.

2.1.6 Verfahren "Haushalts-, Kassen- und Rechnungswesen"

[15] http://www.ldspdm.ldsbb.lvnbb.de/bbi/fach_inf/it/datenschutz/datensch1/lfdlds.htm

[16] s. 4. Tätigkeitsbericht unter 1.4.2 und 6. Tätigkeitsbericht unter 1.4.1.4

Aufgrund der Übertragung von sensiblen personenbezogenen Daten beim Haushalts-, Kassen- und Rechnungswesen-Verfahren (HKR-Verfahren) forderten wir[17], dass bis spätestens zum Ende des Jahres 1999 die per Terminalemulation über das Landesverwaltungsnetz übertragenen Daten verschlüsselt werden.

Vom Landesamt für Datenverarbeitung und Statistik wurde dazu ein Verfahren getestet, das die Verschlüsselung der übertragenen Daten ermöglicht. Als Software kommt die Secure Shell zum Einsatz. Die Länge des asymmetrischen RSA-Schlüssels beträgt dabei 1024 Bit. Durch Nutzung der im HKR-Verfahren schon für den Dateitransfer installierten Verschlüsselungssoftware Pretty Good Privacy (PGP) ist es nun möglich, die gesamte Datenübertragung im HKR-Verfahren zu verschlüsseln. Wir gehen davon aus, dass dieses Verfahren bei allen am HKR-Verfahren beteiligten Stellen nun schnellstmöglich eingeführt wird.

Der Einsatz dieser sicheren Verschlüsselungstechnik wäre auch in anderen Gebieten denkbar. So könnte zum Beispiel auch die Administration von UNIX-Servern über verschlüsselte Verbindungen erfolgen.

Aufgrund der Bemühungen des Landesamt für Datenverarbeitung und Statistik wurde eine Möglichkeit gefunden, die beim HKR-Verfahren übertragenen sensiblen personenbezogenen Daten sicher zu verschlüsseln.

2.1.7 Zertifizierung von öffentlichen Schlüsseln

Vom Landesamt für Datenverarbeitung und Statistik wird schon seit einiger Zeit ein Trust-Center betrieben, in dem u. a. auch die im HKR-Verfahren verwendeten öffentlichen PGP-Schlüssel zertifiziert werden. Öffentliche Schlüssel werden zur Verschlüsselung von Informationen (z. B. E-Mail) oder auch bei der digitalen Signatur benötigt.

Das Landesamt für Datenverarbeitung und Statistik arbeitet derzeit sozusagen als Wurzel-Zertifizierungsstelle des Landes Brandenburg und stellt diese Dienstleistung auch anderen öffentlichen Stellen gegen Entgelt zur Verfügung.

Es muss betont werden, dass das Trust-Center des Landesamtes für Datenverarbeitung und Statistik keine Zertifizierungsstelle im Sinne des Signaturgesetzes ist. Allerdings ist bei der verwaltungsinternen Kommunikation die Verwendung von Signaturschlüsseln, die nicht den hohen verfahrensmäßigen Anforderungen des Signaturgesetzes entsprechen, grundsätzlich hinnehmbar. Bei der Kommunikation zwischen Verwaltung und den Bürgerinnen und Bürgern wie z. B. im "virtuellen Rathaus"[18], sollten dagegen signaturgesetzkonforme Schlüssel angewandt werden. Hierzu gibt es im Landesamt für Datenverarbeitung und Statistik Überlegungen, als

[17] s. 6. Tätigkeitsbericht unter 1.4.1.6

[18] s. Tätigkeitsbericht 1998 unter 2.5

Ausgabestelle für zugelassene private Trustcenter (z. B. des Ostdeutschen Sparkassen- und Giroverbandes) tätig zu werden, in der zertifizierte Chipkarten autorisiert werden. Inwieweit das deutsche Signaturgesetz mit seinen aufwendigen und kostenintensiven Zulassungsverfahren demnächst möglicherweise an die Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[19] angepasst wird, bleibt abzuwarten.

Werden von den öffentlichen Stellen des Landes Verfahren zur digitalen Signatur und zur Verschlüsselung eingesetzt, so sollten die dabei verwendeten öffentlichen Schlüssel vom Trust-Center des Landesamtes für Datenverarbeitung und Statistik zertifiziert werden.

2.2 Neue Orientierung in der Kryptodebatte

In der deutschen Kryptodebatte zeichnet sich eine Trendwende ab. Die Bundesregierung hat mit ihren fünf Eckpunkten zur Kryptopolitik vom 2. Juni 1999 klargestellt, dass kryptographische Verfahren und Produkte ohne Einschränkung entwickelt, vertrieben und genutzt werden dürfen. Sie „sieht in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen“.

[19] Richtlinie vom 3. 12. 1999, ABl. EG

Das Sicherheitsbewusstsein bei den Bürgerinnen und Bürgern, der Wirtschaft und der Verwaltung ist zu schärfen. Die Überprüfbarkeit der Sicherheit von Verschlüsselungsprodukten und die Förderung von offenen Standards für Verschlüsselungssoftware stehen dabei im Vordergrund. Mit ihrer Entschließung vom 7./8. Oktober 1999 haben die Datenschutzbeauftragten von Bund und Ländern[20] diese Absicht der Bundesregierung nachhaltig unterstützt. Sie legen besonderen Wert darauf, dass die europäischen Verschlüsselungsprodukte, deren Algorithmen offen gelegt sind, gefördert werden.

Erwartet wird ferner insbesondere von den öffentlichen Stellen, dass diese mit gutem Beispiel vorangehen und den Einsatz kryptographischer Verfahren zum Schutz personenbezogener Daten häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Weiterhin fordern sie die Hersteller auf, Produkte zu entwickeln, die sicher, leicht bedienbar, im Verbund einsetzbar und kostengünstig sind; erst dann werden die Nutzerinnen und Nutzer in größerem Umfang ihre elektronischen Nachrichten verschlüsseln.

Die Bundesregierung hat mit ihren Eckpunkten der deutschen Kryptopolitik eine gute Ausgangsposition für die Entwicklung und für den Einsatz von starken kryptographischen Verfahren und Produkten geschaffen. Damit kann zukünftig die vertrauliche Verarbeitung und Übertragung von personenbezogenen Daten erheblich verlässlicher als bisher geplant und realisiert werden.

2.3 Biometrie und Datenschutz - Chancen und Risiken

Folgende Szenarien sind denkbar und in absehbarer Zeit auch realisierbar: Wer morgens den Arbeitsplatz betritt, muss nicht mehr den Dienstausweis an der Pforte vorweisen oder das Zeiterfassungssystem bedienen, sondern wird von einer Computerstimme aufgefordert, in die Kamera zu blicken. Kurz darauf öffnet sich die Durchgangstür. Anschließend soll am Arbeitsplatz der PC gestartet werden. Statt nun, wie üblich, das Login-Kennwort und das persönliche Passwort eingeben zu müssen, wird der Zeigefinger in eine kleine Vertiefung auf der Tastatur gelegt, und schon ist der Rechner verfügbar.
Muss man gegenwärtig beim Geldabheben am Geldautomaten zusätzlich zur Geldkarte die persönliche Kennzahl (PIN) eingeben, so könnte dies zukünftig überflüssig werden, wenn etwa Fingerabdruck und Gesichtserkennung miteinander verknüpft werden. Hierzu läuft derzeit das von der Bundesregierung

[20] s. Dokumente zum Datenschutz 1999, Teil A III

geförderte Projekt BioTrust des TeleTrust Deutschland e.V., mit dem der Einsatz von biometrischen Verfahren im Bankenbereich erprobt wird. Private Schusswaffen könnten durch einen eingebauten Fingersensor so gesichert werden, dass unbefugte Personen diese nicht nutzen können. Das Starten des eigenen Autos könnte von einem Fingersensor- oder Spracherkennungssystem abhängig gemacht werden, sodass man keinen Zündschlüssel mehr benötigt. Unbefugte wären vom Lenken des Wagens ausgeschlossen.

Hinter diesen Abläufen verbergen sich folgende Verfahren: Vor der Einlasskontrolle wurden zu einem früheren Zeitpunkt die Gesichtsgeometrien aller Beschäftigten auf einem Computer gespeichert. Bei der aktuellen Kamerakontrolle wird das Gesicht der Person, die Einlass verlangt, mit den gespeicherten Daten der Beschäftigten verglichen; im Falle einer Übereinstimmung wird die Durchgangstür automatisch freigegeben.

Bei der Fingerkontrolle wird ähnlich verfahren, indem die als Referenzmuster früher gespeicherten Fingerdaten der Beschäftigten mit dem auf dem Sensor aufgelegten Finger verglichen werden.

Die beschriebenen Beispiele basieren auf den prinzipiell unveränderlichen physiologischen Merkmalen der betroffenen Person: Ihr Zeigefinger ist einzigartig und unverwechselbar; für das Gesicht gilt dasselbe. Weitere statische Merkmale sind Handabdrücke, die Regenbogenhaut des Auges (Iris) und die Netzhaut (Retina). Sie alle lassen sich für statische biometrische Verfahren nutzen.

Dagegen werden bei dynamischen biometrischen Verfahren keine statischen äußeren Merkmale genutzt, sondern solche, die sich aus der typischen Bewegung und dem typischen Verhalten einer Person ergeben, etwa durch gesprochene Worte, durch die Art, zu schreiben oder die Art, eine Tastatur zu bedienen.

Statische und dynamische biometrische Verfahren können kombiniert werden, um damit die Sicherheit der personenbezogenen Erkennung zu erhöhen.

Generell müsste man sich keine Kenn- und Passworte oder dergleichen mehr merken; die Versuchung, sich wegen der einfacheren Gedächtnisleistung nur triviale Begriffe einzuprägen, bestünde nicht mehr.

Beim derzeitigen Stand der Technik haben die biometrischen Verfahren allerdings noch Unsicherheiten. Es kann zu höheren Fehlerquoten bei der persönlichen Erkennung kommen, weil Personen z. B. ihr Aussehen oder ihre Art, zu schreiben oder zu sprechen, ändern können. Bestimmte Augenmedikamente oder Krankheiten wie Diabetes können zu Veränderungen der Iris bzw. der Netzhaut führen.

Fehlerquoten bei der Erkennung können sowohl zur unberechtigten Abweisung einer befugten Person als auch zur fehlerhaften Anerkennung einer nicht befugten Person führen. In der Praxis wird man die Verfahren so einstellen müssen, dass zwischen diesen beiden Möglichkeiten je nach Sicherheitsbedürfnis ein angemessener Kompromiss erreicht wird.

Biometrische Verfahren sind zudem kriminell angreifbar. Dies hat z. B. im vergangenen Sommer ein Hacker unter den Augen der Öffentlichkeit bewiesen, als er alle bei einem Workshop vorhandenen Fingerabdruck-Scanner zum Narren hielt, indem er sich von den befugten Personen mittels einer Folie Fingerabdrücke besorgte und diese sich auf den eigenen Finger klebte[21]. Auf diese Weise konnte er als Unbefugter in die vorhandenen Systeme eindringen.

Die Anwendung biometrischer Verfahren eröffnet einerseits Chancen für eine Erhöhung der Datensicherheit durch zuverlässige Identifizierung berechtigter Personen. Andererseits birgt sie neue datenschutzrechtliche Risiken, weil sie den Aufbau von Datenbanken mit biometrischen Merkmalen einer Vielzahl von Personen zu Vergleichszwecken voraussetzt, die, einmal vorhanden, auch zu anderen Zwecken eingesetzt werden könnten. Die Befürchtung, der Mensch werde immer lückenloser überwacht, erhält damit neue Nahrung.

Um Missbrauch zu begegnen, bedarf es klarer rechtlicher Grenzen: Jede personenbezogene Datenverarbeitung hat sich an den verfassungsrechtlichen Werten der Menschenwürde und des informationellen Selbstbestimmungsrechts zu orientieren. Auch die Maßgaben der Verhältnismäßigkeit, der Datenvermeidung und Datensparsamkeit sind zu berücksichtigen. Ferner dürfen gespeicherte Daten nur eingeschränkt mit anderen personenbezogenen Informationen verknüpft werden, da die Speicherung des Abbilds der Gesamtheit einer Persönlichkeit gegen das Prinzip der Menschenwürde verstößt und immer unzulässig ist.

Der Einsatz biometrischer Verfahren etwa zur Aufdeckung des Mehrfachbezugs von Sozialhilfe würde dagegen eine vollständige und routinemäßige erkennungsdienstliche Behandlung aller Personen voraussetzen, die Unterstützung beim Sozialamt beantragen. Ein solcher Generalverdacht des Unterstützungsbetruges wäre nicht mit dem Menschenbild des Sozialstaats vereinbar, sodass auch der Gesetzgeber, der eine entsprechende Regelung ins Auge fassen würde, an verfassungsrechtliche Grenzen stieße.

Die Erhebung biometrischer personenbezogener Merkmale darf stets nur mit Wissen und Einwilligung der Betroffenen erfolgen. Befinden sich die Betroffenen in einem Abhängigkeitsverhältnis, das eine freie Entscheidung über die Einwilligung erschwert (z. B. im Arbeits- oder Dienstverhältnis), ist eine gesetzliche Grundlage etwa in dem längst überfälligen Arbeitnehmerdatenschutzgesetz erforderlich.

---

[21] s. c`t 17/1999, S. 34

In technisch-organisatorischer Hinsicht sollten biometrische Verfahren, soweit ihr Einsatz rechtlich zulässig ist, in datenschutzfreundlicher Form angewandt werden.

Biometrische Verfahren können sowohl „Fluch“ als auch „Segen“ für das Persönlichkeitsrecht der Betroffenen sein. Bei einer datenschutzgemäßen und vernünftigen Anwendung werden sie sich zukünftig im Alltag durchsetzen.

3 Telekommunikation und Medien

3.1 Das Telekommunikationsgeheimnis - ein Eckstein der Informationsgesellschaft

Das Fernmeldegeheimnis wird im Grundgesetz (Art. 10) ebenso wie in der Brandenburgischen Landesverfassung (Art. 16) als Menschenrecht garantiert. Dieses Menschenrecht gewinnt vor dem Hintergrund der geradezu atemberaubenden Entwicklung neuer Informations- und Kommunikationstechniken eine ganz neue Bedeutung. Immer mehr nutzen die Bürgerinnen und Bürger angesichts sinkender Tarife sowohl das herkömmliche Sprachtelefon als auch das Telefax und zunehmend das Internet zum Austausch elektronischer Nachrichten. Die herkömmliche Briefpost ("Snail-Mail", Schneckenpost) wird durch die elektronische Post (E-Mail) ergänzt und teilweise auch ersetzt. Insbesondere Wirtschaftsunternehmen tauschen zunehmend sensible Informationen online aus. Mobiltelefone werden immer häufiger genutzt, wobei die Fest- und Mobilfunknetze alsbald zusammenwachsen werden. Die Informationsgesellschaft ist ohne Telekommunikation undenkbar.

Vor diesem Hintergrund sind die Aussagen bedeutsam, die das Bundesverfassungsgericht in seinem Urteil vom Juli 1999 zur verdachtslosen Rasterfahndung des Bundesnachrichtendienstes in der satellitengestützten Telekommunikation gemacht hat[22]. Zwar wurden die Befugnisse des Bundesnachrichtendienstes im Grundsatz als verfassungsgemäß angesehen, im Einzelnen wurde der Schutz personenbezogener Daten bei solchen Maßnahmen aber auch verstärkt. Von grundsätzlicher Bedeutung sind aber die Ausführungen, die das Gericht zur Bedeutung des Telekommunikationsgeheimnisses für die Informationsgesellschaft gemacht hat. Es hebt hervor, dass die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlungen und weiteren Verwendung durch andere Behörden schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen führen kann. Dabei sei nicht nur

[22] BVerfG, Urteil vom 14.7.1999 - 1 BvR 226/94 u. a. - EuGRZ 1999 S. 389 ff.

die individuelle Beeinträchtigung einer Vielzahl einzelner Grundrechtsträger zu berücksichtigen, sondern die heimliche Überwachung des Fernmeldeverkehrs betreffe auch die Kommunikation der Gesellschaft insgesamt[23].

Dieser Zusammenhang, den das Bundesverfassungsgericht zu Recht hervorgehoben hat, ist bisher zu wenig beachtet worden. Zwar gibt es schon seit langem gesetzliche Befugnisse zum Abhören von Telefongesprächen zur Bekämpfung bestimmter Straftaten, deren Liste allerdings ständig erweitert worden ist. Vor allem aber die noch vor dem Hintergrund der analogen Vermittlungstechnik formulierte gesetzliche Befugnis zur Auswertung von Verbindungsdaten im Fernmeldeanlagengesetz (§ 12) hat inzwischen durch die Digitalisierung der Telekommunikationsnetze eine verfassungsrechtlich problematische Qualität erhalten. Dennoch hat der Bundesgesetzgeber die Geltung dieser Vorschrift im Berichtszeitraum nochmals bis Ende des Jahres 2001 verlängert[24], anstatt zumindest eine den Eingriffsschwellen bei Abhörmaßnahmen entsprechende Befugnis in die Strafprozessordnung aufzunehmen, wie es die Datenschutzbeauftragten des Bundes und der Länder gefordert haben[25]. Lediglich die Löschungs- und Benachrichtigungspflicht bei Abhörmaßnahmen ist auf die Auswertung der Verbindungsdaten erstreckt worden.

---

23 BVerfG a. a. O. S. 409

24 Artikel 4 des Gesetzes zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20.12.1999, BGBl. I S. 2492

25 Zuletzt in der Konferenzentschließung vom 08.10.1999, s. Dokumente zum Datenschutz 1999, Teil A III

Von Bedeutung ist die genannte Entscheidung des Bundesverfassungsgerichts auch deshalb, weil darin die Sicherung der freien Telekommunikation als Teil des Grundrechtsschutzes bezeichnet wird, der sich nicht auf eine Abschirmung des Kommunikationsinhaltes gegen staatliche Kenntnisnahme beschränkt, sondern auch die Umstände der Kommunikation schützt, also insbesondere die Tatsache, ob, wann und wie oft zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist. Mit den Worten des Gerichts: "Die Nutzung des Kommunikationsmediums soll in allem vertraulich möglich sein"[26]. Schließlich erstreckt sich das Telekommunikationsgeheimnis auch auf die Verwendung von Daten, die durch rechtmäßige Abhörmaßnahmen erhoben worden sind. Gerade in diesem Bereich hat das Gericht noch erhebliche Kontrolllücken festgestellt, die geschlossen werden müssen[27].

Vor diesem Hintergrund hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht gemeinsam mit den Datenschutzbeauftragten der Länder Berlin, Bremen, Nordrhein-Westfalen und Schleswig-Holstein eine Trendwende in der Telekommunikationspolitik gefordert[28]. Angesichts einer Verdoppelung der Zahl der Telefonüberwachungen zwischen 1995 und 1998 bundesweit ist es dringend geboten, die Effektivität solcher Maßnahmen kritisch zu untersuchen. Da das von der Verfassung garantierte Recht der Einzelnen, prinzipiell unkontrolliert elektronisch zu kommunizieren, unverzichtbare Grundvoraussetzung einer offenen, demokratischen Informationsgesellschaft ist, haben die fünf Datenschutzbeauftragten ein umfassendes Gesetz zur Sicherung der freien Telekommunikation gefordert, das folgende Kernpunkte enthalten sollte:

- Verpflichtung aller Telekommunikationsanbieter zu Datensparsamkeit und Datenvermeidung;

- Verschlüsselung als kostenlose Standardleistung;

- Einführung eines Mediennutzungsgeheimnisses, damit die neuen Medien ebenso unkontrolliert genutzt werden können wie Zeitung, Buch oder Fernsehen;

- Begrenzung der Mitwirkungspflichten bei Abhörmaßnahmen auf lizenzpflichtige Unternehmen (z. B. Telefongesellschaften);

- regelmäßige und unabhängige Evaluation der staatlichen Überwachungspraxis;

---

[26] BVerfG a. a. O. S. 402

[27] s. o. 1.1

[28] Für eine Sicherung der freien Telekommunikation in unserer Gesellschaft, s. Dokumente zum Datenschutz 1999, Teil B

- Förderung datenschutzfreundlicher Techniken;

- wirksamer Schutz beruflicher Schweigepflichten, z. B. von Ärztinnen und Ärzten oder Anwältinnen und Anwälten und

- Stärkung des strafrechtlichen Schutzes für das Kommunikationsgeheimnis durch stärkere polizeiliche Prävention gegen illegales Abhören, Prüfung eines Verbots des freien Verkaufs von Abhörtechnik und effektivere Strafverfolgung illegaler Abhörmaßnahmen.

Insgesamt muss verhindert werden, dass das Telekommunikationsnetz durch eine Erweiterung staatlicher Befugnisse zu einer überwachungsgeneigten Infrastruktur wird. Anderenfalls wäre eine entscheidende Voraussetzung für das nötige Vertrauen der Bürgerinnen und Bürger in der entstehenden Informationsgesellschaft gefährdet.

3.2 Entwurf zum Datenschutz in der Telekommunikation mit Defiziten

Seit In-Kraft-Treten des Telekommunikationsgesetzes Anfang 1998 ist die Neufassung der Rechtsverordnung zum Datenschutz in der Telekommunikation überfällig. Im Berichtszeitraum legte das Bundeswirtschaftsministerium zunächst einen entsprechenden Entwurf vor, der die maximale Frist zur Speicherung von Verbindungsdaten gegenüber dem bisherigen Rechtszustand auf bis zu drei Jahre verlängert hätte. Hiergegen haben sich die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom März 1999 entschieden gewandt[29]. Mittlerweile liegt ein überarbeiteter Verordnungsentwurf vor, der die Kritik der Datenschutzbeauftragten insoweit aufgreift, als Verbindungsdaten nur sechs Monate lang nach dem Ende der Verbindung gespeichert bleiben dürfen.

Allerdings enthält auch der neue Entwurf eine Reihe von Defiziten, auf die wir das Wirtschaftsministerium hingewiesen haben. So werden das bisherige Wahlrecht der Kundinnen und Kunden zwischen verschiedenen Formen der Speicherung von Verbindungsdaten (vollständige Speicherung oder Löschung mit Rechnungsversand) auf das Verhältnis zum rechnungsstellenden Diensteanbieter begrenzt. Dies hätte zur Folge, dass die Verbindungsdaten bei allen übrigen Diensteanbietern, die im liberalisierten Telekommunikationsmarkt solche Daten im Rahmen von Zusammenschaltungsvereinbarungen oder bei der Abrechnung von Call-by-Call-Verbindungen speichern, unabhängig von der Entscheidung der Kundin oder des Kunden stets bis zu sechs Monate nach Beendigung der Verbindung dort gespeichert blieben. Damit würde der gegenwärtige Datenschutzstandard für die Nutzerinnen und Nutzer erheblich abgesenkt, was der Geltung des Telekommunikationsgeheimnisses für die näheren Umstände der

[29] s. Dokumente zum Datenschutz 1999, Teil A I

Kommunikation nicht genügt. Zudem müssen auch die Diensteanbieter, die nicht selbst Rechnungen stellen, ein Interesse daran haben, das klare, Rechtssicherheit schaffende Regelungen über die Dauer der zulässigen Speicherung von Verbindungsdaten in ihrem Bereich getroffen werden, die zugleich der Präferenz der Kundinnen und Kunden entsprechen.

Außerdem soll das Verfahren zum Schutz von Beratungsstellen nach dem Verordnungsentwurf noch weniger praktikabel geregelt werden als nach geltendem Recht. Vorzuziehen wäre eine Regelung nach dem sog. holländischen Modell, bei dem niemand mit seiner Rufnummer ohne ausdrückliche Einwilligung in Einzelverbindungsnachweise aufgenommen wird. Auch die geplante Regelung zur Rasterung der Verbindungsdatenbestände für Zwecke der Missbrauchsbekämpfung würde zu gravierenden Verschlechterungen gegenüber dem geltenden Recht führen. Die Vorentwürfe hatten noch die Nutzung von anonymisierten oder pseudonymisierten Daten für diese Zwecke vorgesehen, wobei im Einzelfall auf die erforderlichen personenbezogenen Daten unter bestimmten Voraussetzungen zugriffen werden könnte. Diese Regelung sollte wieder aufgegriffen werden.

Auch rückwirkende Fangschaltungen will der Verordnungsentwurf ermöglichen, ohne dass diese Rasterung der Verbindungsdaten auf bestimmte gravierende Fälle beschränkt würde.

Schließlich sollen die bisherigen Rechte der Bürgerinnen und Bürger, einer Invers-Auskunft (Telefonnummer ist bekannt, Inhaber des dazugehörigen Anschlusses wird gesucht) zu widersprechen und die Eintragung des Widerspruchs gegen die Aufnahme in elektronische Verzeichnisse (z. B. auf CD-ROM) in das gedruckte Telefonbuch zu verlangen, ohne plausiblen Grund entfallen.

Es bleibt zu hoffen, dass unsere Vorschläge zur notwendigen Verbesserung des Entwurfs spätestens im Bundesrat berücksichtigt werden, ohne dessen Zustimmung die Verordnung nicht in Kraft treten kann.

3.3 Unzulässiger Umgang mit Verbindungsdaten

3.3.1 Speicherung von Verbindungsdaten und Kontrolle der Bediensteten

Das Telekommunikationsgeheimnis ist auch im Verhältnis zwischen Dienstbehörden und öffentlichen Bediensteten zu beachten. Das gilt insbesondere (aber nicht nur) dann, wenn die Dienstbehörde ihren Mitarbeiterinnen und Mitarbeitern die Nutzung der dienstlichen Telefonanlage für private Zwecke gestattet. Andererseits hat die Dienstbehörde ein Interesse daran, eine korrekte Abrechnung von Privatgesprächen sicherzustellen. Vor diesem

Hintergrund haben wir im Berichtszeitraum mehrere Nebenstellenanlagen (TK-Anlagen) in Behörden Brandenburgs eingehend technisch und organisatorisch überprüft und mussten in zwei Fällen datenschutzrechtliche Mängel beanstanden, andererseits konnten wir aber auch positive Entwicklungen feststellen.

Die TK-Anlage einer Behörde war so programmiert, dass bei der Amtseinwahl zwischen dienstlichen und privaten Gesprächen differenziert werden musste. Bei dienstlichen Gesprächen war für die Freischaltung der Amtsleitung die Vorwahl "0" zu wählen, bei privaten Gesprächen die Vorwahl "8".

Nach einer Anordnung des Behördenleiters wurden bei Dienstgesprächen Datum und Uhrzeit des Anrufs, Nebenstellennummer, vollständige Zielrufnummer sowie die verbrauchten Tarifeinheiten erfasst. Diese Daten wurden von allen Dienstgesprächen längstens vier Monate vollständig gespeichert. Die vollständige Speicherung der genannten Verbindungsdaten über einen längeren Zeitraum erfolgte insbesondere zu dem Zweck, stichprobenartige Kontrollen der dienstlich geführten Gespräche dahingehend vorzunehmen, ob auch private Gespräche über die Vorwahl "0" geführt wurden.

Die stichprobenartigen Kontrollen wurden in der Art durchgeführt, dass aus dem aufgelaufenen Gesamtdatenbestand per Zufall fünf zu überprüfende Beschäftigte ausgewählt wurden. Bei diesen Beschäftigten wurden dann rückwirkend anhand der gespeicherten Verbindungsdaten die dienstlichen Telefonate überprüft.

Das oben beschriebene Verfahren führt dazu, dass Verbindungsdaten einer großen Zahl von Beschäftigten gespeichert werden, bei denen die stichprobenartige Kontrolle nicht durchgeführt wird. Die Speicherung ist daher nicht erforderlich. Sie widerspricht zudem den für alle Landesbehörden verbindlichen Dienstanschlussvorschriften (DAV)[30], die der Minister der Finanzen 1993 erlassen hat. Dieser Erlass legt den zulässigen Umfang der Verarbeitung von Verbindungsdaten fest und konkretisiert damit das verfassungsrechtliche Telekommunikationsgeheimnis für den Bereich der Landesverwaltung.

Nach den DAV ist es zwar zulässig, die oben genannten Verbindungsdaten zu erheben, um das konkrete Telefongespräch oder die Faxverbindung technisch zu ermöglichen. Nach Beendigung der Verbindung, d. h. unmittelbar nach dem Auflegen, sind jedoch alle Daten zu löschen. Eine Ausnahme besteht nur insoweit, als die Daten für die stichprobenartige Überprüfung der dienstlichen Gespräche erforderlich sind. Eine generelle Speicherung aller Verbindungsdaten bei Dienstgesprächen über den Zeitpunkt nach Beenden der Verbindung hinaus ist damit rechtswidrig.

[30] Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg

Die DAV lassen aber durchaus eine effektive Kostenkontrolle bei dienstlich geführten Gesprächen zu. Sofern es für notwendig erachtet wird, solche stichprobenartige Überprüfungen vorzunehmen, sehen die DAV folgendes Verfahren vor: Zunächst sind per Zufallsprinzip die in Zukunft zu überprüfenden Nebenstellen auszuwählen. Erst dann dürfen die Verbindungsdaten der von diesen Nebenstellen geführten Dienstgespräche für einen möglichst kurz zu haltenden Zeitraum gespeichert werden. Die Verbindungsdaten bei allen übrigen Nebenstellen sind unverzüglich nach Gesprächsende zu löschen.

Teilweise lässt es die Software nicht zu, dass nur die Verbindungsdaten bestimmter Nebenstellen gespeichert werden. Dies gilt vor allem bei solchen TK-Anlagen, die vor In-Kraft-Treten der DAV installiert wurden. In diesen Fällen sollte kurzfristig die alte Software angepasst oder durch neue ersetzt werden. Für die Zwischenzeit sollte auf die stichprobenartigen Kontrollen verzichtet und alle Verbindungsdaten nach Gesprächsende gelöscht werden.

Die oben beschriebene rechtswidrige Speicherung von Verbindungsdaten bei der kontrollierten Behörde war ein so erheblicher Mangel, dass wir eine förmliche Beanstandung gegenüber dem zuständigen Ministerium für Stadtentwicklung, Wohnen und Verkehr aussprechen mussten.

Im Zusammenhang mit der Bearbeitung einer Eingabe stellten wir bei einem Finanzamt weitere Verstöße gegen die DAV durch unzulässige Speicherungen von Verbindungsdaten fest und beanstandeten dies gegenüber dem Ministerium der Finanzen. Die Stellungnahme des Ministeriums ließ die Schlussfolgerung zu, dass mehrere Finanzämter in Brandenburg für ihre internen TK-Anlagen die gleiche Software zur Gebührendatenverarbeitung nutzen und deshalb in ähnlicher Weise rechtswidrig verfahren. So werden neben weiteren Mängeln u. a. vollständige Verbindungsdaten für alle dienstlichen Gespräche langfristig gespeichert, weil eine Festlegung zufälliger Stichproben für die Missbrauchskontrolle vor Beginn des Abrechnungszeitraumes nicht erfolgen kann. Mehrere telefonische Hinweise bei uns und die Kontrolle eines weiteren Finanzamtes bestätigten unsere Vermutung. So wurden in den letzten zwei bis drei Jahren für mehrere Finanzämter noch neue nicht mit den Festlegungen in der DAV konforme TK-Anlagen angeschafft, obwohl die DAV bereits seit 1993 in Kraft ist.

Die Finanzämter lehnen zum Teil jede Verantwortung für die Beschaffung der nicht datenschutzgerechten TK-Anlagen ab, da diese von den zuständigen Landesbauämtern ohne ausreichende Beteiligung der betreffenden Finanzämter vorgenommen wurden. Demgegenüber müssen wir darauf hinweisen, dass jedes Finanzamt als eigene Daten verarbeitende Stelle selbst die Verantwortung für die Verarbeitung personenbezogener Daten trägt. Damit verbunden ist natürlich, dass sich die Finanzämter bereits bei der Auswahl der betreffenden Software den erforderlichen Einfluss sichern müssen.

Da es sich bei der Gebührendatenverarbeitung für TK-Anlagen aber um ein automatisiertes Verfahren i. S. v. § 7 Abs. 3 des Brandenburgischen Datenschutzgesetzes handelt, fällt hier auch dem Ministerium der Finanzen, das als oberste Landesbehörde für die schriftliche Freigabe des Verfahrens zuständig ist, eine wesentliche Verantwortung zu. Denn spätestens vor der Verfahrensfreigabe hätten entsprechende Prüfungen zu der Erkenntnis führen müssen, dass die betreffende Software zur Gebührendatenverarbeitung eine datenschutzgerechte Arbeitsweise wie sie in der DAV vorgeschrieben wird, nicht zulässt und damit ungeeignet ist.

Dass die Verfahrensfreigabe durch das Ministeriums der Finanzen trotz der offensichtlichen Mängel erfolgte, ist für uns unverständlich, da wir in der Vergangenheit gerade im Ministerium der Finanzen einen vorbildlichen Umgang mit personenbezogenen Daten bei der Gebührenabrechnung innerhalb des TK-Verbundes der obersten Landesbehörden feststellen konnten. Ein positives Beispiel dafür wird unter Punkt 3.3.3 beschrieben, wo das Landesbauamt Brandenburg die Abnahme der neuen TK-Anlage im Landesbehördenzentrum Brandenburg, an die im Übrigen auch die Telefone des dortigen Finanzamtes angeschlossen sind, solange verweigerte, bis die dazugehörige Software zur Gebührendatenverarbeitung durch Nachbesserung die datenschutzrechtlichen Forderungen der DAV erfüllen konnte.

Immerhin hat auch das Ministerium der Finanzen die Anschaffung einer neuen Software für die Gebührendatenverarbeitung angekündigt und zugesichert, dass bis zu diesem Zeitpunkt keine dienstlichen Verbindungsdaten mehr gespeichert werden. Besonders zu begrüßen ist auch, dass von der Oberfinanzdirektion Cottbus bereits unmittelbar nach unserem Kontrollbesuch durch ein Rundschreiben alle Finanzämter des Landes Brandenburg auf die bestehenden Mängel der Software hingewiesen wurden.

Verbindungsdaten dienstlicher Gespräche sind unmittelbar nach Gesprächsende zu löschen, es sei denn, sie sind zur Durchführung stichprobenartiger Kontrollen erforderlich. Daten über Privatgespräche sind nach Abrechnung, spätestens aber nach zwei Monaten zu löschen.

3.3.2 Unzulässige Datenspeicherung führt zum Verlust des Arbeitsplatzes

An uns wandte sich eine Petentin, die in einem Brandenburger Finanzamt nach einer umfangreichen Qualifizierung in das Beamtenverhältnis auf Probe berufen werden sollte. Vor Beginn der Probezeit kamen dem Vorgesetzten aber Bedenken hinsichtlich der charakterlichen Eignung der Anwärterin und von einer Berufung in das Beamtenverhältnis auf Probe wurde abgerückt. Damit lief der befristete Arbeitsvertrag der Petentin automatisch aus, und sie verlor ihre Beschäftigung.

Woraus ergab sich die angebliche charakterliche Nichteignung der Petentin, als Beamtin im Land Brandenburg tätig zu werden? Zwei Vermerken über Aussprachen mit der Petentin war zu entnehmen, dass ihr vorgeworfen wurde, Privatgespräche über die dienstliche Telekommunikationsanlage ohne ordnungsgemäße Bezahlung geführt zu haben. Dabei ging es um einen Gesamtbetrag von 47,12 DM in fünf aufeinander folgenden Monaten, der sich noch erheblich reduzierte, da bei mehreren Telefongesprächen eine eindeutige Zuordnung zum privaten Bereich nicht vorgenommen werden konnte. Die Gespräche hatten nach Angaben der Petentin überwiegend dienstlichen Charakter. Der Petentin wurden Verbindungsdaten vorgehalten, die - wie das Ministerium der Finanzen inzwischen selbst eingeräumt hat - längst hätten gelöscht sein müssen.

Die gesamte Verbindungsdatenspeicherung in dieser Behörde war zu beanstanden[31]. Darüber hinaus wurden anhand der vollständigen Verbindungsdaten die verwandtschaftlichen oder sonstige Beziehungen der Petentin zu den angerufenen Personen ermittelt und in den Akten festgehalten, um den Vorwurf nicht korrekt abgerechneter Privatgespräche zu untermauern und zugleich zu klären, ob eine unerlaubte Hilfeleistung in Steuersachen vorlag.

Der Fall zeigt anschaulich, mit welch gravierenden Konsequenzen moderne Telefonnebenstellenanlagen zur Kontrolle der Mitarbeiterinnen und Mitarbeiter zweckentfremdet werden können. Dennoch wurde unsere Anregung, kurzfristig zu prüfen, wie berufliche Nachteile für die Petentin durch die unzulässige Datenverarbeitung im betreffenden Finanzamt vermieden werden können, nicht aufgegriffen.

Ob die Entscheidung der Dienstbehörde, rechtswidrig gespeicherte Verbindungsdaten in dieser Weise trotz des vergleichsweise geringen Betrages zu Lasten der Petentin zu verwerten, einer arbeitsgerichtlichen Überprüfung standhielte, ist zweifelhaft.

Mit den Dienstanschlussvorschriften, aber auch mit zahlreichen Dienstvereinbarungen ist es unvereinbar, wenn die in TK-Anlagen verarbeiteten Daten zu Verhaltens- und Leistungskontrollen der Beschäftigten verwendet werden.

3.3.3 Datenschutzfreundliche TK-Anlage im Landesbehördenzentrum Brandenburg

Kurz nach Erlass der Dienstanschlussvorschriften stellten wir im Jahre 1994 fest, dass die im Landesamt zur Regelung offener Vermögensfragen Brandenburg bereits früher in Betrieb genommene TK-Anlage bezüglich der Speicherung von Verbindungsdaten nicht den Forderungen der Dienstanschlussvorschriften entsprach und deshalb nur eine Dienstvereinbarung mit dem Personalrat abgeschlossen werden konnte, die datenschutzrechtlich weit hinter der vom Ministerium der Finanzen entworfenen Musterdienstvereinbarung, für alle Landesbehörden, zurückblieb. Das

[31] s. o. 3.3.1

Ministerium stimmte deshalb der Erneuerung der Software zur Gebührendatenverarbeitung im Rahmen der ohnehin erforderlichen Umbau- und Erweiterungsmaßnahmen zu, und als Übergangslösung vereinbarten wir mit dem Landesamt zur Regelung offener Vermögensfragen bis zum Einsatz der neuen Software besondere technisch-organisatorische Maßnahmen, die einen Zugriff auf die unrechtmäßig gespeicherten Verbindungsdaten nur unter direkter Beteiligung des Personalrates ermöglichten.

In der Folgezeit bezog uns das für die Beschaffung der neuen TK-Anlage zuständige Landesbauamt Brandenburg in die Ausschreibung und Abnahme der neuen Software zur Gebührendatenverarbeitung ein. Dem konsequenten Vorgehen der Bediensteten des Landesbauamtes Brandenburg ist es zu verdanken, dass im Landesbehördenzentrum Brandenburg ein Verfahren zur Gebührendatenverarbeitung eingesetzt wird, das alle Forderungen der Dienstanschlussvorschriften in vorbildlicher Weise erfüllt. Angewandt wird die Software VARIX COUNT der Firma DeTeWe. In Zusammenarbeit mit dem Softwarehersteller entstand darüber hinaus eine moderne Lösungsvariante, die unabhängig von der jeweiligen TK-Anlage selbst arbeitet und deren Schnittstelle an nahezu alle Anlagen der gängigen Hersteller angepasst werden kann.

Um auch für die Zukunft zu sichern, dass im Land Brandenburg nur mit den Festlegungen in der Dienstanschlussvorschrift konforme TK-Anlagen angeschafft werden, haben wir gemeinsam mit dem Ministerium der Finanzen einen Forderungskatalog zum Datenschutz erarbeitet, der künftig bereits in die Ausschreibungsunterlagen für neue TK-Anlagen aufgenommen werden soll.

Die öffentlichen Stellen des Landes sollten ihre Telefonnebenstellenanlagen, soweit sie den Datenschutz nicht hinreichend berücksichtigen, so bald wie möglich mit datenschutzfreundlicher Technik ausstatten, die inzwischen verfügbar ist.

3.3.4 Private Telefongespräche per Chipkarte

Unter Leitung des Landesamtes für Datenverarbeitung und Statistik wird gegenwärtig in einer Arbeitsgruppe Telekommunikation, in der einige Ministerien und auch unsere Behörde mitarbeiten, ein Konzept zur effektiveren Abrechnung privater Telefonate im Kommunikationsverbund der obersten Landesbehörden erstellt. Das Ziel ist, ein Verfahren zu finden, welches kostengünstiger und zugleich datenschutzfreundlicher betrieben werden kann.

Erste Überlegungen gehen davon aus, dass ein Chipkarten gestütztes Verfahren zum Einsatz kommt. Alle Bediensteten würden eine Chipkarte erhalten, mit der sie im Voraus an einem Bargeldterminal ihr zentral geführtes Konto aufladen können. Die Chipkarte wird dabei als Identifikationsmedium verwendet. Mit der Einführung der

Chipkarten-Lösung müsste auch jeder Mitarbeiterin und jedem Mitarbeiter eine 6-stellige PIN zugeordnet werden. Vor einem privaten Telefongespräch geben die Bediensteten an ihrem Apparat zuerst die Kennziffer für private Telefonate ein, dann die PIN und im Anschluss daran die gewünschte Telefonnummer. Während des Telefonats werden vom Kontostand der Anruferin oder des Anrufers die vertelefonierten Einheiten abgezogen. Bei Unterschreitung eines bestimmten Kontostandes (z. B. 2 Euro), kann die Nebenstelle so konfiguriert werden, dass die anrufende Person automatisch (z. B. durch ein akustisches Signal) darüber informiert wird. Es besteht u. a. auch die Möglichkeit, den aktuellen Kontostand über das Telefon abzufragen.

Da die Bediensteten in der TK-Anlage über ihre PIN identifiziert werden können, besteht auch weiterhin die Möglichkeit, auf Wunsch Einzelverbindungsnachweise zu erstellen. Der größte Vorteil des Verfahrens besteht jedoch darin, dass die nachträgliche Abrechnung privater Telefonate komplett entfallen würde und damit die laufenden Kosten und die zu verarbeitenden personenbezogenen Daten reduziert werden könnten. Es bleibt zu hoffen, dass dieses datenschutzfreundliche Verfahren möglichst schnell in die Praxis umgesetzt wird.

Die Einführung eines Chipkarten gestützten Verfahrens zur effektiveren Abrechnung privater Telefonate im Kommunikationsverbund der obersten Landesbehörden ist zu begrüßen, da damit auch weniger personenbezogene Daten als bisher verarbeitet werden würden. Auf diese Weise könnte dem Gebot der Datensparsamkeit im Brandenburgischen Datenschutzgesetz entsprochen werden.

3.4 Datenverarbeitung beim Rundfunk

3.4.1 Datenschutzkontrolle beim Ostdeutschen Rundfunk Brandenburg neu geregelt

Auf Vorschlag des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht[32] hat der Landtag im ORB-Änderungsgesetz vom 7. April 1999 die Datenschutzkontrolle beim Ostdeutschen Rundfunk Brandenburg (ORB) in der Weise neu geregelt, dass der Landesbeauftragte die Verarbeitung personenbezogener Daten im administrativ-wirtschaftlichen Bereich und die Datenschutzbeauftragte des ORB die Datenverarbeitung im journalistisch-redaktionellen Bereich der Rundfunkanstalt kontrolliert. Damit ist insbesondere die Verarbeitung der Daten von Fernsehzuschauerinnen und -zuschauern bzw. Radiohörerinnen und -hörer im Zusammenhang mit dem Einzug der Rundfunkgebühren erstmals einer unabhängigen Datenschutzkontrolle unterworfen. Soweit es um den Datenschutz bei der Verwendung personenbezogener Daten beim ORB für eigene publizistische Zwecke, also z. B. bei der Programmgestaltung, geht, bleibt die Datenschutzbeauftragte des ORB Ansprechpartnerin.

[32] vgl. Tätigkeitsbericht 1998, Pkt. 3.3.2

3.4.2 "Haben Sie wirklich noch keinen Fernseher?"

Allen die in Brandenburg ein Radio- und/oder ein Fernsehgerät zum Empfang bereit halten, müssen an den ORB Rundfunkgebühren zahlen. Der ORB hat mit dem Einzug der Gebühren die Gebühreneinzugszentrale (GEZ) beauftragt. Wer nur ein Radiogerät angemeldet hat, bezahlt eine geringere Gebühr als diejenigen, die auch ein Fernsehgerät zum Empfang bereit halten.

Um festzustellen, ob solche Rundfunkteilnehmerinnen und Rundfunkteilnehmer, die nur ein Radio angemeldet haben, auch noch einen Fernseher besitzen, lässt der ORB in regelmäßigen Abständen von der GEZ sogenannte Mailing-Aktionen durchführen.

Der ORB ist der Auffassung, dass die angeschriebenen Personen dazu verpflichtet sind, ausdrücklich mitzuteilen, wenn dies nicht der Fall ist. Die Verpflichtung zu einer solchen Negativauskunft leitet der ORB aus dem zwischen den Bundesländern geschlossenen Rundfunkgebührenstaatsvertrag ab, nach dessen Wortlaut der ORB bzw. die von ihm beauftragte GEZ von Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie ein Rundfunkempfangsgerät zum Empfang bereithalten und dies nicht oder nicht umfassend angemeldet haben, Auskunft über diejenigen Tatsachen verlangen kann, die Grund, Höhe und Zeitraum ihrer Gebührenpflicht betreffen. Der ORB ist der Ansicht, dass es sich hier um eine Auskunft über den Grund der Gebührenpflicht handele, die für die Bestandspflege seiner Daten erforderlich sei.

Wir teilen die Auffassung des ORB nicht. Unstreitig ist dabei zunächst, dass selbstverständlich auch Personen, die nur ein Hörfunkgerät angemeldet haben, Rundfunkteilnehmer im Sinne des Rundfunkgebührenstaatsvertrages sind und somit grundsätzlich auch Auskunft erteilen müssen.

Die Auskunftspflicht knüpft nach dem Staatsvertrag aber an die Gebührenpflicht an. Hat jemand also nur ein Radio, ist er auch nur dafür gebühren- und auskunftspflichtig. Folglich ist niemand verpflichtet anzugeben, dass er kein Fernsehgerät zum Empfang bereit hält.

Etwas anderes gilt nur dann, wenn tatsächliche Anhaltspunkte vorliegen, dass ein Hörfunkteilnehmer auch ein Fernsehgerät zum Empfang bereit hält und dieses nicht ordnungsgemäß bei der GEZ angemeldet hat. Außerdem sind natürlich alle "Nur-Radiohörer", die einen Fernseher erwerben, verpflichtet, diesen von sich aus anzumelden.

Die Pflicht, der vom ORB beauftragten GEZ Auskünfte zu erteilen, besteht nur, soweit auch eine Gebührenpflicht besteht. Hat jemand nur ein Radio angemeldet und hält keinen Fernseher zum Empfang bereit, so ist er nicht verpflichtet, diesen Umstand der GEZ in Form einer "Negativauskunft" mitzuteilen.

3.4.3 Verfahren bei der Rundfunkgebührenbefreiung

Die derzeit geltende Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht (Rundfunkgebührenbefreiungsverordnung - RfGebBefrVO) sieht vor, dass Rundfunkteilnehmerinnen und -teilnehmer aus sozialen Gründen oder aufgrund einer Behinderung von der Rundfunkgebühr befreit werden können.

Das Verfahren sieht vor, dass die betroffene Person einen Antrag auf Rundfunkgebührenbefreiung bei ihrem örtlichen Sozialamt stellen muss. Über diesen Antrag entscheidet der ORB, nachdem ihm das Sozialamt einen Entscheidungsvorschlag gemacht hat.

Dieses Verfahren ist nicht datenschutzgerecht. Es führt dazu, dass sehr sensible Daten über die sozialen oder gesundheitlichen Verhältnisse von Bürgerinnen und Bürgern ohne Not zwei öffentlichen Stellen zur Kenntnis gelangen, obwohl nur eine - der ORB - letztlich die Entscheidung zu treffen hat.

Zudem ist bei diesem Verfahren seit Jahren die rechtliche Einordnung der Datenweitergabe vom Sozialamt an den ORB ungeklärt. Das Erarbeiten eines Entscheidungsvorschlags durch das Sozialamt kann jedenfalls nicht als Datenverarbeitung im Auftrag angesehen werden. Diese Tätigkeit setzt eine eigenständige Prüfung des Sozialamtes voraus, so dass bereits eine Funktionsübertragung vorliegt. Demzufolge ist die Datenweitergabe aus unserer Sicht eine Datenübermittlung, wobei fragwürdig ist, ob diese erforderlich ist.

Das Verfahren sollte vielmehr so gestaltet werden, dass entweder das Sozialamt oder der ORB allein über die Befreiung von der Rundfunkgebühr entscheiden. Bei der von uns bevorzugten ersten Variante müsste dann geregelt werden, dass nur die Tatsache der Rundfunkgebührenbefreiung, nicht aber der Befreiungsgrund dem ORB übermittelt werden darf.

Nachdem bereits im Jahre 1997 die Novellierung der Rundfunkgebührenbefreiungsverordnung im Gespräch war, seitdem aber kein Fortgang in dieser Angelegenheit verzeichnet werden konnte, haben wir die Staatskanzlei erneut gebeten, sich für eine Novellierung der Verordnung in unserem Sinne einzusetzen.

Die Staatskanzlei hat uns daraufhin mitgeteilt, dass beabsichtigt sei, die Thematik im Rahmen eines voraussichtlich im Jahre 2001 zu verabschiedenden 5. Rundfunkänderungsstaatsvertrages erneut aufzugreifen.

4 Inneres

4.1 Polizei

4.1.1 Schleierfahndung

Im vergangenen Jahr sind auch in Brandenburg die unter dem Namen "Schleierfahndung" besser bekannten Befugnisse zu "lagebildabhängigen" [33] - und damit verdachtsunabhängigen - Kontrollen für die Polizei eingeführt worden. Obwohl wir uns grundsätzlich gegen die Schleierfahndung ausgesprochen haben, weil mit der Befugniserweiterung zwangsläufig das Risiko der unverdächtigen Bürgerinnen und Bürger erhöht wird, staatliche Informationseingriffe hinnehmen zu müssen, haben wir im Gesetzgebungsverfahren dennoch Formulierungsvorschläge vorgelegt, die den Datenschutzstandard verbessern sollten. Sie sind bei der Novellierung nicht berücksichtigt worden.

4.1.1.1 Novellierung des Polizeigesetzes

[33] *Lagebild: Beschreibung des örtlich und zeitlich bestimmten Kriminalitätsaufkommens*

Zur Einführung der Befugnis zu lagebildabhängigen Kontrollen ist das Brandenburgische Polizeigesetz (BbgPolG) um eine Regelung (§ 11 Abs. 3) ergänzt worden, die festlegt, das jedermann - also nicht nur Störer oder Notstandspflichtige - im öffentlichen Verkehrsraum befragt und mitsamt den mitgeführten Sachen in Augenschein genommen werden darf, sowie sich ausweisen muss, wenn der Polizei Lageerkenntnisse vorliegen, dass Straftaten von erheblicher Bedeutung begangen werden sollen[34]. Ort, Zeit und Umfang der Maßnahme dürfen nur durch den Polizeipräsidenten oder seinen Vertreter im Amt angeordnet werden.

Darüber hinaus ist die Befugnis zur Identitätsfeststellung (§ 12 BbgPolG) dahingehend erweitert worden, dass die Polizei ebenso wie der Bundesgrenzschutz die Befugnis hat, zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität und zur Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug jedermann im 30 km breiten Abstandsstreifen von der Bundesgrenze zu kontrollieren. Bei dieser Kontrolle ist wiederum jedermann verpflichtet, sich auszuweisen, ohne selbst dafür einen Anlass gegeben zu haben. Wer dies nicht kann, weil sie oder er die Personalpapiere nicht dabei hat, muss gewärtigen, zur nächsten Polizeiwache mitgenommen und erkennungsdienstlich behandelt zu werden, wenn die Polizei auf andere Weise ihre oder seine Identität nicht feststellen kann (§ 13 Abs. 2 BbgPolG).

Im Herbst 1999 hat das Landesverfassungsgericht Mecklenburg-Vorpommern in einem bundesweit beachteten Urteil eine in das dortige Polizeigesetz aufgenommene Befugnis zur Schleierfahndung auf Durchgangsstraßen zwar für unvereinbar mit dem Grundrecht auf informationelle Selbstbestimmung erklärt, solche Maßnahmen im 30-km-Grenzstreifen dagegen als zulässig betrachtet[35]. Zugleich hat das Gericht aber wegen des Ausnahmecharakters der Identitätsfeststellung auch in Grenznähe alle weiteren Folgeeingriffe zu deren Durchsetzung, also insbesondere Freiheitsentziehung (Mitnahme zur Wache) und die erkennungsdienstliche Behandlung solange für unzulässig erklärt, bis der Gesetzgeber die erforderlichen bereichsspezifischen Regelungen hierfür getroffen hat. Auch für die Speicherung und weitere Verwendung der bei dieser Gelegenheit erhobenen Daten über Nicht-Verdächtige könne nicht auf die vorhandenen allgemeinen Datenverarbeitungsbefugnisse zurückgegriffen werden.

Auch wenn das geänderte Brandenburgische Polizeigesetz anders als das entsprechende Gesetz im nördlichen Nachbarland eine Schleierfahndung nicht auf Durchgangsstraßen, sondern nur im Gebiet der Bundesgrenze bis zu einer Tiefe von 30 km zulässt, sollte geprüft werden, ob das Urteil des Landesverfassungsgerichts Mecklenburg-Vorpommern nicht auch Konsequenzen für das Polizeirecht im Land Brandenburg hat.

4.1.1.2 Praktische Umsetzung

---

[34] 1. Gesetz zur Änderung des Gesetzes über die Aufgaben und Befugnisse der Polizei im Land Brandenburg vom 20.05.1999, GVBl. I S. 171

[35] Urteil vom 21.10.1999 - LVerfG 2/98

Unterdessen haben brandenburgische Polizeidienststellen mehrere Schleierfahndungen durchgeführt. Das der jeweiligen Maßnahme zu Grunde liegende Lagebild enthielt - wie in § 11 Abs. 3 BbgPolG vorgeschrieben - Anhaltspunkte dafür, dass innerhalb eines bestimmten Zeitraums am Kontrollort Straftaten begangen werden sollten.

Die Polizei dokumentiert lediglich die Gesamtzahl der angehaltenen Personen bzw. Fahrzeuge sowie der "Treffer", d. h. der festgestellten Verstöße gegen Rechtsvorschriften. In wie vielen Fällen die angehaltenen Personen nicht nur befragt wurden, sondern sich ausweisen oder sich und ihre mitgeführten Sachen durchsuchen lassen mussten, wird nicht vermerkt.

4.1.1.3 Evaluation tut Not

Wir hatten uns im Gesetzgebungsverfahren für eine Befristung der Befugnis zu verdachtsunabhängigen Kontrollen entsprechend dem Bundesgrenzschutzgesetz eingesetzt, um auch die praktischen Erfahrungen mit den erweiterten Befugnissen der Polizei evaluieren zu können. Dem hat das Ministerium des Innern entgegengehalten, auch der Verzicht auf eine Befristung stehe einer angemessenen Evaluierung nicht entgegen. Für eine aussagekräftige Evaluierung müssen die Anzahl der von der Maßnahme Betroffenen sowie die Art der Eingriffe (Befragung, Vorzeigen der Ausweispapiere bis zur erkennungsdienstlichen Behandlung) vermerkt werden. Sie sollten anschließend von unabhängiger Seite im Hinblick darauf ausgewertet werden, ob die neuen Befugnisse der Polizei die erwarteten Erfolge gezeitigt haben. Wenn der Gesetzgeber feststellt, dass sich gesetzliche Eingriffsbefugnisse in Grundrechte der Bürgerinnen und Bürger als ungeeignet erweisen, um das angestrebte Ziel zu erreichen, ist er von Verfassungs wegen gehalten, diese Eingriffsbefugnisse kritisch zu überprüfen und, falls nötig, rückgängig zu machen.

4.1.2 Der Große Lauschangriff vor den Verfassungsgerichten

Seit 1996 enthält das Brandenburgische Polizeigesetz (BbgPolG) Befugnisse zum verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes und zur Anfertigung von Bildaufzeichnungen und Bildaufnahmen in oder aus Wohnungen (§ 33 Abs.3 und 4 BbgPolG), die im Berichtszeitraum erstmals angewandt worden sind[36]. Im vergangenen Jahr hat - unabhängig davon - das Verfassungsgericht des Landes Brandenburg diese Befugnisse im Wesentlichen für verfassungskonform erklärt[37].

---

[36] s. Pkt. 4.1.4.6

[37] Urteil vom 30.06.1999 - VfGBbg 3/98 -; die Entscheiidungsformel ist mit Gesetzeskraft bekanntgemacht im GVBl. S. 273 f.

Auch wenn das Verfassungsgericht damit nicht den grundsätzlichen Einwänden gefolgt ist, die der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht im Gesetzgebungsverfahren gegen die Befugnis zum polizeilichen Lauschangriff erhoben hatte[38], so sind doch die zahlreichen einschränkenden Maßgaben bemerkenswert, die das Gericht für die Anwendung dieser Befugnis gesetzt und von denen es seine Bewertung abhängig gemacht hat.

So hat es betont, dass der Begriff der Kontakt- und Begleitpersonen von Verfassungs wegen eng auszulegen sei und Überwachungsmaßnahmen gegen diesen Personenkreis noch strengeren Voraussetzungen unterliegen als Maßnahmen gegen den potentiellen Straftäter selbst. Technische Mittel dürfen verdeckt nur gegen solche Personen eingesetzt werden, zu denen der potentielle Straftäter in Bezug auf die konkrete Straftat in Verbindung steht. Die gesetzliche Pflicht, diese Personen nach Abschluss der Maßnahme zu benachrichtigen, sobald die Datenerhebung dadurch nicht mehr gefährdet wird, hat eine wesentliche grundrechtssichernde Bedeutung und muss - über den Wortlaut des Gesetzes hinaus - auch auf unbeteiligte Personen erstreckt werden, die zwangsläufig mitbeobachtet worden sind. Träger von Amts- und Berufsgeheimnissen (z. B. Ärztinnen und Ärzte, Anwältinnen und Anwälte) gehören nicht zu den Kontakt- und Begleitpersonen, gegen die verdeckte technische Mittel eingesetzt werden dürfen.

Maßnahmen der "akustischen Wohnraumüberwachung" (Lauschangriffe) sind nur in der Wohnung des potentiellen Straftäters oder seiner Kontakt- und Begleitpersonen zur Bekämpfung organisierter Schwerkriminalität zulässig, wobei auch hier Träger von Berufsgeheimnissen im Rahmen des Vertrauensverhältnisses mit ihnen nicht zu den Kontakt- und Begleitpersonen gezählt werden dürfen. Das Gericht hat ausdrücklich betont, dass der Gesetzgeber sich mit dieser Regelung an der Grenze dessen bewegt, was von Verfassungs wegen noch als zulässige Einschränkung des grundrechtlichen Freiheitsraums hingenommen werden kann. Im Interesse des Schutzes der Allgemeinheit vor schwerster Kriminalität und unter den genannten Eingriffsvoraussetzungen erscheint die Regelung dem Gericht aber als "verfassungsrechtlich noch hinnehmbar".

Das Verfassungsgericht des Landes Brandenburg musste bei seiner Entscheidung auch der Tatsache Rechnung tragen, dass der Bundesgesetzgeber mit der Einführung des Großen Lauschangriffs und der entsprechenden Änderung des Grundrechts auf Unverletzlichkeit der Wohnung im Grundgesetz (Art. 13) im März 1998 den Schutz vor heimlicher Wohnraumüberwachung zwar bundesweit eingeschränkt, gegenüber dem Art. 15 der Brandenburgischen Landesverfassung aber erhöht hat. Insofern ist der weiterreichende Schutz durch das Bundesgrundrecht auch bei Anwendung des Brandenburgischen Polizeigesetzes zu berücksichtigen. Das Landesverfassungsgericht hat hier ebenfalls durch eine grundgesetzkonforme Auslegung des Gesetzes gewisse

[38] s. unter 4. Tätigkeitsbericht Pkt. 3.2.1.1

Korrekturen vorgenommen. Der Landesgesetzgeber hat nun zu prüfen, inwieweit dies zu Änderungen des Polizeigesetzes führen muss.

Letztlich wird sich aber die Übereinstimmung der Befugnisse im Brandenburgischen Polizeigesetz mit Art. 13 Grundgesetz danach richten, ob die bundesgesetzlichen Regelungen zum Großen Lauschangriff ihrerseits mit dem Grundgesetz vereinbar sind. Zur Entscheidung darüber ist das Bundesverfassungsgericht im Berichtszeitraum angerufen worden; die Entscheidung steht allerdings noch aus.

4.1.3 "Deutsch-Russisches Regierungsabkommen - Daten für die Mafia?"

Mit diesem reißerischen Titel war ein Presseartikel über das Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Russischen Föderation über die Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung überschrieben[39]. Unabhängig davon, ob die russischen Datenempfänger nun tatsächlich mafiose Strukturen aufweisen, ist festzustellen, dass datenschutzrechtliche Bestimmungen in das Abkommen kaum Eingang gefunden haben.

Mit dem noch nicht in Kraft getretenen Abkommen sollen gemeinsame Maßnahmen der zuständigen russischen und deutschen Behörden zur Bekämpfung von Straftaten von erheblicher Bedeutung, wie z. B. Handel mit Menschen, Waffen und Drogen, Erpressung, Geldwäsche, Herstellen und Verbreiten von Falschgeld sowie Terrorismus ermöglicht werden. Dazu sollen u. a. die zur Verhütung, Ermittlung und Aufklärung der Straftaten erforderlichen Daten ausgetauscht werden. Zur Erleichterung der Zusammenarbeit ist ferner vorgesehen, Verbindungsbeamte in die jeweiligen Länder zu entsenden. Unter den in dem Abkommen aufgeführten "zuständigen" Behörden wird auch der Föderale Sicherheitsdienst der Russischen Föderation genannt, der zwar auch polizeiliche Aufgaben wahrnimmt, im Wesentlichen aber als Inlandsgeheimdienst tätig ist.

Noch ehe uns die Landesregierung den Text des Abkommens zur Stellungnahme zugeschickt hatte, haben wir sowohl dem Innen- als auch dem Justizministerium unsere datenschutzrechtlichen Bedenken vorgetragen. Ungeachtet der Bedeutung, die der Bekämpfung der grenzüberschreitenden Kriminalität gerade auch im Verhältnis zu Russland beizumessen ist, muss sie in den Schranken der deutschen Rechtsordnung erfolgen. Insbesondere zwei Gründe lassen dies jedoch bei dem vorliegenden Abkommen zweifelhaft erscheinen.

---

[39] *Der Spiegel 28/1999 S. 30 ff.*

Zum einen soll die Zweckbindung personenbezogener Daten, die zwischen den beiden Ländern ausgetauscht werden, stärker als zulässig durchbrochen werden. Sie können ganz allgemein zur Bekämpfung von Straftaten von erheblicher Bedeutung und zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit genutzt werden, auch wenn sie ursprünglich zu einem ganz anderen Zweck übermittelt worden sind. Dies entspricht nicht dem Bundeskriminalamtsgesetz (BKAG), in dem die strikte Zweckbindung der konkreten Datenübermittlung festgelegt ist und auf die der Empfänger ausdrücklich hingewiesen werden muss (§ 14 Abs. 7 BKAG). Das Brandenburgische Polizeigesetz lässt Übermittlungen ins Ausland nicht zu, wenn Grund zu der Annahme besteht, dass gegen den Zweck eines deutschen Gesetzes, insbesondere im Hinblick auf Speicherungs-, Nutzungs- oder Übermittlungsbeschränkungen sowie Löschungsverpflichtungen verstoßen wird oder schutzwürdige Belange der Betroffenen beeinträchtigt werden. Eine solche Beeinträchtigung entsteht vor allem dann, wenn nicht nur Daten Verdächtiger, sondern auch von Opfern, Zeugen, Kontakt- und Auskunftspersonen oder von sog. anderen Personen übermittelt werden sollen.

Zum anderen enthält das Abkommen keine Regelungen über die Überwachung der datenschutzrechtlichen Vorschriften des Abkommens in der Russischen Föderation. Zwar ist Russland seit 1996 Mitglied des Europarates, hat aber die Konvention zum Schutz personenbezogener Daten bisher nicht ratifiziert. Hinzu kommt, dass die Russische Föderation weder eine Datenschutzgesetzgebung noch einen Datenschutzbeauftragten kennt.

Wir haben den zuständigen Ministerien Gespräche angeboten, um die datenschutzrechtlichen Probleme des Abkommens zu erörtern. Das Justizministerium hat mitgeteilt, dass das Abkommen zunächst noch innerhalb der Landesregierung geprüft werde und vorgeschlagen, das Gespräch erst danach aufzunehmen.

Unterdessen hat die Ständige Vertragskommission der Länder das Abkommen beraten. Auf der Sitzung im vergangenen Jahr haben auch die Vertreter mehrerer Bundesländer - darunter Brandenburg - datenschutzrechtliche Bedenken vorgetragen und die Zustimmung ihrer Länder verweigert. Damit ist das Abkommen bisher lediglich zur Kenntnis genommen worden. Jetzt ist man im Bundesinnenministerium zu der Überzeugung gelangt, dass ein formales Ratifizierungsverfahren erforderlich ist und hat mit der Ausarbeitung des Gesetzentwurfs begonnen.

4.1.4 Querschnittsprüfung beim polizeilichen Staatsschutz

Bereits im letzten Berichtszeitraum haben wir im Brandenburgischen Landeskriminalamt (LKA) mit der Querschnittsprüfung des polizeilichen Staatsschutzes begonnen und sie vergangenes Jahr in einem Polizeipräsidium fortgesetzt.

4.1.4.1 Aufgaben des Staatsschutzes

Auf Präsidiumsebene ist der Staatsschutz zuständig für die Gefahrenabwehr im Bereich politisch motivierter Straftaten sowie für die Erforschung und vorbeugende Bekämpfung von Staatsschutzdelikten, die im Präsidiumsbereich anfallen und bei denen keine zentrale Strafverfolgung durch das Landeskriminalamt geboten ist (§ 5 und § 8 Brandenburgisches Polizeiorganisationsgesetz (POGBbg)).

Dem Staatsschutz im Brandenburgischen Landeskriminalamt ist die Erforschung und vorbeugende Bekämpfung u. a. von Fällen terroristischer Gewaltkriminalität, politisch motivierter, organisiert begangener Kriminalität, von Landesverrat- und Sabotagedelikten sowie von Straftaten der Gefährdung der äußeren Sicherheit zugewiesen. Er hat darüber hinaus die Aufgabe, alle für die polizeiliche Verhütung und Verfolgung in diesen Bereichen "bedeutsamen" Informationen zu sammeln und auszuwerten. Das Landeskriminalamt ist die Verbindungsstelle zu den beim Bundeskriminalamt betriebenen Staatsschutzverbunddateien insbesondere zur Arbeitsdatei "PIOS - Innere Sicherheit" (APIS), auf die die Staatsschutzabteilungen der Polizeipräsidien keinen unmittelbaren Zugriff haben. Darüber hinaus werden dort Gefährdungsermittlungen und Lagebeurteilungen erstellt und Gefährdungsermittlungen bei denjenigen durchgeführt, die eines Personenschutzes bedürfen (§ 10 POGBbg).

4.1.4.2 Materiell-rechtliche Grundlagen

Im Bereich der Gefahrenabwehr unterliegt der Staatsschutz den Vorschriften des Brandenburgischen Polizeigesetzes[40]. Rechtliche Grundlage für den Bereich der Strafverfolgung ist die Strafprozessordnung, ggf. in Verbindung mit dem Brandenburgischen Datenschutzgesetz. Damit hat der Staatsschutz keine allgemeine Vorfeldkompetenz, die ihn befugen würde, personenbezogene Informationen losgelöst von gefahrenbegründenden Tatsachen zu verarbeiten. Eingriffe in das informationelle Selbstbestimmungsrecht setzen immer entweder den Anfangsverdacht für eine begangene Straftat oder eine polizeiliche Gefahr voraus.

[40] vom 19.3.1996 GVBl. I S. 74, geänd. am 30.5.1999 GVBl. I S. 171

Da Polizei und Verfassungsschutz sich häufig mit derselben Klientel befassen, kommt der strikten Aufgabentrennung zwischen beiden Stellen im Bereich Staatsschutz besondere Bedeutung zu. Der Verfassungsschutz darf gemäß §§ 3 ff. Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG) Informationen über politisch motivierte Gruppierungen oder Bestrebungen, die sich gegen die freiheitlich demokratische Grundordnung oder die Sicherheit des Bundes oder eines Landes richten, sammeln. Im Gegensatz dazu darf die Informationsverarbeitung des Staatsschutzes erst einsetzen, wenn ein Anfangsverdacht oder eine polizeiliche Gefahr vorliegt.

Die strikte Aufgabentrennung zwischen Polizei und Verfassungsschutz muss vor allen Dingen beim Einsatz der besonderen Erhebungsmethoden nach dem Polizeigesetz berücksichtigt werden, da hier die Staatsschutzabteilungen und die Verfassungsschutzbehörde weitgehend das gleiche Instrumentarium, aber eben zur Erfüllung unterschiedlicher Aufgaben und nach unterschiedlichen rechtlichen Vorgaben einsetzen dürfen. Das ausdrückliche Verbot der Brandenburgischen Verfassung, im Wege der Amtshilfe Maßnahmen, die dem Verfassungsschutz nicht zustehen, durch die Polizei zu veranlassen (Art. 11 Abs. 3), macht eine gründliche Prüfung der jeweiligen Einsatzvoraussetzungen notwendig.

Das Trennungsgebot muss auch bei der weiteren Datenverarbeitung beachtet werden. Rechtsgrundlage für die Datenübermittlung der Polizei an die Verfassungsschutzbehörde ist § 14 BbgVerfSchG. Die Vorschrift verpflichtet alle Behörden des Landes, von sich aus der Verfassungsschutzbehörde Informationen über verfassungsschutzrelevante gewaltgeneigte Bestrebungen und Einzelpersonen zu übermitteln. Darüber hinaus müssen die Polizeibehörden auch Informationen über nichtgewaltgeneigte verfassungsschutzrelevante Bestrebungen übermitteln, wenn ihnen tatsächliche Anhaltspunkte vorliegen, dass die Daten für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich sind. Daraus ergibt sich, dass die Übermittlung von Daten über Personen, die lediglich polizeipflichtig sind (§§ 5,6 und 7 BbgPolG), unzulässig ist.

Im Polizeigesetz ist ergänzend festgelegt, dass Daten von Kontakt-, Begleit- und Auskunftspersonen nur an Polizeibehörden und damit nicht an den Verfassungsschutz übermittelt werden dürfen (§ 41 Abs. 1. Satz 3 BbgPolG), weil bei diesem Personenkreis die vorhandenen Anhaltspunkte als nicht ausreichend angesehen werden. Der Verfassungsschutzbehörde entstehen dadurch keine unbehebbaren Informationsverluste, da sie bei entsprechenden Hinweisen auf eine verfassungsschutzrelevante Bestrebung den betreffenden Personenkreis selbst mit den ihr zur Verfügung stehenden Befugnissen beobachten kann.

Brandenburgisches Polizeigesetz und Strafprozessordnung zielen nicht auf eine Registrierung einer Person oder einer Gruppierung als Ganzes, sondern auf die Erfassung von relevanten Sachverhalten. Die Erstellung von Persönlichkeitsbildern durch Informationen über das sonstige, nicht sachverhaltsbezogene Umfeld ist unzulässig.

Informationen über legale, besonders geschützte Grundrechtsausübungen wie Meinungsäußerungen oder die Teilnahme an einer Demonstration dürfen auch dann nicht gespeichert werden, wenn bereits rechtmäßige Informationssammlungen über die Betroffenen vorhanden sind.

Auch bei Staatsschutzdelikten gelten die besonders hohen Übermittlungsvoraussetzungen für Daten von Kontakt- und Begleitpersonen bzw. sog. anderen Personen. Sie dürfen nur an Polizeibehörden, nicht aber an den Verfassungsschutz übermittelt werden.

4.1.4.3 Arbeitsdatei PIOS - Innere Sicherheit (APIS)

Die Arbeitsdatei PIOS - Innere Sicherheit (APIS) ist eine beim Bundeskriminalamt betriebene Verbunddatei, die den Länderpolizeien und dem Bundeskriminalamt für die Speicherung von Daten über Personen zur Verfügung steht, die bei der Ermittlung von Staatsschutzdelikten als Tatverdächtige, Beschuldigte, Kontakt- und Begleitpersonen oder Gefährder bekannt werden. Anhand der Errichtungsanordnung, mit einem umfangreichen Katalog APIS-relevanter Straftaten, darunter nicht nur die eigentlichen Staatsschutzdelikte sondern auch andere mit Staatsschutzbezug, entscheiden die Staatsschutzabteilungen der Polizeipräsidien selbst, ob die Voraussetzungen für eine Speicherung der Betroffenen in der Datei vorliegen und melden die Daten an das Landeskriminalamt. Erst dort werden die Daten nach einer weiteren Prüfung in APIS eingestellt.

Ebenso wie bei Kriminalakten und anderen Dateien muss die Polizei auch bei Speicherungen in APIS in regelmäßigen Abständen prüfen, ob der Datensatz für die weitere Aufgabenerfüllung der Polizei noch erforderlich ist. Dazu übermittelt das Bundeskriminalamt dem Landeskriminalamt Listen mit denjenigen Datensätzen, bei denen eine Erforderlichkeitsprüfung ansteht. Wir haben festgestellt, dass in der Regel eine Prüffrist von 5 Jahren vergeben wird und damit die erste Erforderlichkeitsprüfung nach 5 Jahren fällig ist.

Dies halten wir für zu lang und haben empfohlen, für Fälle von geringerer Bedeutung - hier vor allem bei einem Tatvorwurf im Zusammenhang mit dem "Tragen verfassungswidriger Kennzeichen" (§ 86 a Strafgesetzbuch) - eine zweijährige Prüffrist festzusetzen. Das Landeskriminalamt folgt dieser Empfehlung bisher nicht.

4.1.4.4 Prüfung von APIS-Akten und Kriminalakten

Bei der Prüfung der Unterlagen haben wir festgestellt, dass einzelne Betroffene als Tatverdächtige in APIS registriert sind und eine Kriminalakte zu ihrer Person geführt wird, weil sie einer Gruppe zugerechnet wurden, aus der heraus verfassungswidrige Kennzeichen öffentlich gezeigt oder verfassungswidrige Parolen gerufen wurden, ohne dass ihnen die Tat selbst zugerechnet werden konnte.

In solchen Fällen haben wir empfohlen, die APIS-Speicherung mit dem Ziel der Löschung zu prüfen, weil wir meinen, dass nicht genügend Anhaltspunkte vorhanden sind, um die Speicherung aufrecht zu erhalten.

Auch hier ist das Landeskriminalamt nicht bereit, unsere Empfehlung umzusetzen.

4.1.4.5 Prüfung der Staatsschutzkriminalakten und Gruppenvorgänge in einem Polizeipräsidium

Bei der Prüfung einzelner, zufällig ausgewählter Akten eines Polizeipräsidiums haben wir u. a. folgende Mängel festgestellt und das Präsidium um Stellungnahme gebeten:

Mitteilungen der Staatsanwaltschaft über den Verfahrensausgang

In allen überprüften Kriminalakten fanden sich Mitteilungen der Staatsanwaltschaft über eine Verfahrenseinstellung ohne Angabe der Rechtsgrundlage der Einstellung (s. unten Pkt. 5.1). In solchen Fällen hat das Polizeipräsidium das zu jeder Straftat in der Kriminalakte befindliche sog. Merkblatt lediglich durchgestrichen und mit der angehefteten Mitteilung in der Kriminalakte belassen. Dies ist nur für eine Übergangszeit hinnehmbar. Eine dauernde Aufbewahrung der Merkblätter, ohne dass die Rechtsgrundlage der Verfahrenseinstellung bei der Staatsanwaltschaft erfragt wurde, ist unzulässig.

Aussonderungsprüfdatum

Bei der Anlage einzelner Kriminalakten waren anscheinend zwei- oder sogar fünfjährige Aussonderungsprüffristen vergeben worden. Dies entspricht nicht § 37 BbgPolG i. V. m. den Richtlinien zu der Datei "Kriminalaktennachweis-Brandenburg" (KAN-BB). Das Brandenburgische Polizeigesetz schreibt vor, dass für automatisierte Dateien Prüffristen festzulegen sind, zu denen spätestens überprüft werden muss, ob die Daten zur Aufgabenerfüllung der Brandenburgischen Polizei weiterhin erforderlich sind. In der Richtlinie ist die erste Prüffrist auf ein Jahr festgesetzt, d. h. dass in Brandenburg ein Jahr nach dem Anlegen der Kriminalakte und der Speicherung im KAN-BB die Erforderlichkeitsprüfung fällig ist. Erst danach kann im Einzelfall eine Aufbewahrungsfrist von zwei oder fünf Jahren festgesetzt werden.

Speicherung von Nichtstörern in Gruppenvorgängen

In den Vorgängen, die der Staatsschutz des Polizeipräsidiums zu Personenzusammenschlüssen führt, fanden sich personenbezogene Daten von Kfz-Haltern, deren Kennzeichen an gefahrenrelevanten Orten notiert worden waren, um anschließend die Fahrzeughalter zu ermitteln. Dabei gibt es keine Personalienfeststellung der Fahrer, so dass durch die Maßnahme nicht ermittelt werden kann, ob der Halter überhaupt vor Ort gewesen ist. Dessen ungeachtet enthielten die Akten aber nicht nur die Daten derjenigen Betroffenen, die bereits in der Vergangenheit als Störer polizeilich bekannt geworden waren, sondern auch die Daten derjenigen Halter, die zuvor nicht als Störer aufgefallen waren.

Während eine kurzfristige Aufbewahrung der Daten derjenigen Betroffenen hinnehmbar ist, bei denen der Abgleich mit den kriminalpolizeilichen Sammlungen ermittlungsrelevante Erkenntnisse ergibt, gilt dies nicht für die Daten der Nichtstörer. Gem. §§ 5 und 6 BbgPolG sind Maßnahmen nur gegen solche Personen zulässig, die eine Gefahr verursachen. Daraus lässt sich nicht die auch nur vorübergehende Aufbewahrung personenbezogener Daten in solchen Fällen ableiten, in denen es selbst nach einem Datenabgleich keine Anhaltspunkte für eine Störereigenschaft der Betroffenen gibt.

Wir haben gefordert, dass Listen mit Halterdaten, die bei den oben dargestellten polizeilichen Maßnahmen erhoben werden, von vornherein nicht in den Gruppenvorgängen abgelegt werden dürfen. Sie müssen sofort nach Ablauf der Maßnahme - also der Halterabfrage und anschließenden Recherche in polizeilichen Datensammlungen - vernichtet

werden. Die Gruppenvorgänge dürfen nur diejenigen Halterdaten einschließlich Kfz-Kennzeichen enthalten, bei denen durch die Dateienrecherche ermittlungsrelevante Erkenntnisse angefallen sind.

4.1.4.6 Prüfung der Datenverarbeitung im Zusammenhang mit einer langfristigen Observation

In einem Polizeipräsidium ist eine langfristige Observation gem. § 32 BbgPolG verbunden mit verdeckten Videoaufzeichnungen gem. § 33 Abs. 1 BbgPolG - also außerhalb der Wohnung des Betroffenen - sowie ein verdecktes Abhören und Aufzeichnen des gesprochenen Wortes in der Wohnung gem. § 33 Abs. 3 BbgPolG durchgeführt worden.

Die grundrechtssichernden Verfahrensschritte waren eingehalten worden. So war die langfristige Observation gem. § 32 Abs. 2 BbgPolG zunächst vom Behördenleiter und die darauffolgenden Verlängerungen vom zuständigen Amtsgericht angeordnet worden. Das Landgericht war auch beim Großen Lauschangriff dem ausführlich begründeten Antrag des Polizeipräsidenten zunächst gefolgt, eine Verlängerung hat es aber - auch vor dem Hintergrund des zwischenzeitlich ergangenen Urteils des Brandenburgischen Verfassungsgerichts vom Juni 1999[41] - abgelehnt. Die in § 32 Abs. 3 bzw. § 33 Abs. 7 BbgPolG vorgeschriebene Benachrichtigung der Betroffenen, die nach Abschluss der Maßnahme erfolgen muss, sobald der Zweck der Datenerhebung nicht mehr gefährdet werden kann, war zum Zeitpunkt der Prüfung bereits eingeleitet worden. Bezüglich der o. g. Sachverhalte hat die Prüfung keine datenschutzrechtlichen Mängel ergeben.

Anders verhält es sich mit der Nutzung der im Zuge der Observation und der verdeckten Bildaufzeichnung erstellten Unterlagen. Obwohl sie personenbezogene Daten über die dort als Kontakt- bzw. Begleitpersonen Bezeichneten sowie über Dritte enthielten, waren sie nicht nur an Polizeibehörden übermittelt worden. Dies widerspricht § 41 BbgPolG (s. oben Pkt. 4.1.4.1).

Die Übersendung der Unterlagen an andere als Polizeibehörden ohne vorheriges Unkenntlichmachen der personenbezogenen Daten dieses Personenkreises stellt einen erheblichen Verstoß gegen datenschutzrechtliche Bestimmungen dar. Diesen Verstoß habe ich gegenüber dem Ministerium des Innern beanstandet.

---

[41] VfGBbg 3/98; s. dazu Pkt. 4.1.2

Eine rechtswidrige Nutzung der Unterlagen zum großen Lauschangriff hat es nach unseren Erkenntnissen nicht gegeben.

Die im Zusammenhang mit der Observation, der verdeckten Bildaufzeichnung und dem Großen Lauschangriff erstellten Unterlagen sind unterdessen mit Ausnahme der Anträge auf richterliche Anordnung sowie der Benachrichtigungen an die Betroffenen im Polizeipräsidium vernichtet worden.

4.2 Verfassungsschutz

Erst zum Datenschutzbeauftragten

Vor einigen Jahren hatte ein Petent bei der Verfassungsschutzbehörde ein Auskunftsersuchen gestellt und die Mitteilung erhalten, dass er dort wegen des Verdachts, an Straftaten mit extremistischer Motivation beteiligt gewesen zu sein, erfasst sei. Da alle gegen ihn anhängigen Ermittlungsverfahren von der Staatsanwaltschaft eingestellt worden waren, weil die Ermittlungen nicht genügend Anhaltspunkte für die Eröffnung des gerichtlichen Verfahrens ergeben hatten, hielt der Petent die Datenspeicherung bei der Brandenburgischen Verfassungsschutzbehörde für unrechtmäßig und klagte vor dem Verwaltungsgericht auf Löschung der Erkenntnisse. Das Verwaltungsgericht gab seiner Klage in zwei Punkten statt und verpflichtete die Brandenburgische Verfassungsschutzbehörde zur Datenlöschung. In einem Punkt allerdings ist die Klage zurückgewiesen worden.

Seine zum Teil abweisende Entscheidung stützt das Verwaltungsgericht auf § 12 Abs. 3 Satz 3 Brandenburgisches Verfassungsschutzgesetz. Danach kann die Verfassungsschutzbehörde die Auskunftserteilung gegenüber dem Petenten ohne Angabe von Gründen ablehnen. Sie muss die Betroffenen aber auf ihr Recht hinweisen, sich an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu wenden, (was hier geschehen war). Erst dem Landesbeauftragten für den Datenschutz müssen die Erkenntnisse zugänglich gemacht werden. Er ist aber nicht berechtigt, seinerseits nun dem Antragsteller die Auskunft zu erteilen, die der Verfassungsschutz zuvor verweigert hatte. Seine Mitteilung muss vielmehr so formuliert sein, dass der Antragsteller zwar über die Prüfung und die datenschutzrechtliche Beurteilung informiert wird, daraus jedoch keine Rückschlüsse über den Erkenntnisstand bei der Verfassungsschutzbehörde ziehen kann. Jede weitergehende Auskunft bedarf der Zustimmung des Verfassungsschutzes. Weiterhin kann der Datenschutzbeauftragte die Parlamentarische

Kontrollkommission in denjenigen Fällen einschalten, bei denen zwischen ihm und der Verfassungsschutzbehörde unterschiedliche Auffassungen über die Rechtmäßigkeit der Datenverarbeitung bestehen.

Diese relativ weitgehenden Kontrollbefugnisse des Datenschutzbeauftragten müssen erst ausgeschöpft sein, ehe die Betroffenen ihren Auskunfts- und Löschungsanspruch auf dem Rechtsweg durchzusetzen versuchen. Bei Auskunftsverweigerung durch den Verfassungsschutz müssen Betroffene sich nach Auffassung des Verwaltungsgerichts zunächst an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht wenden, "bevor sie gerichtliche Hilfe in Anspruch nehmen können"[42].

Im Fall des Petenten, haben wir unterdessen die in Rede stehenden Erkenntnisse geprüft und dem Petenten mitgeteilt, dass wir keine datenschutzrechtlichen Einwände gegen die Auskunftsverweigerung erheben können. Dies gilt jedoch nicht für die weitere Speicherung. Wir haben daher die Brandenburgische Verfassungsschutzbehörde gebeten, uns zu erläutern, inwieweit die in Rede stehende Erkenntnis zur weiteren Aufgabenerfüllung der Verfassungsschutzbehörde erforderlich ist. Eine Stellungnahme der Verfassungsschutzbehörde steht noch aus.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht soll im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen zum Grundrechtsschutz beitragen[43].

4.3 Meldewesen

4.3.1 Meldedaten an die DVU trotz Widerspruchs

Im Vorfeld der Landtagswahl haben sich zahlreiche Bürgerinnen und Bürger an unsere Behörde gewandt, weil ihnen von der Partei "Deutsche Volksunion" (DVU) direkt an sie adressierte Wahlwerbung zugesandt worden war. Die meisten Betroffenen waren Einwohnerinnen und Einwohner der Landeshauptstadt Potsdam, die angaben, sie hätten bereits vor Jahren beim Einwohnermeldeamt Widerspruch gegen die Weitergabe ihres Namens und ihrer Anschrift an Parteien eingelegt.

---

42 Urteil vom 30.03.1999, Verwaltungsgericht Potsdam, Az.: 3 K 198/97

43 So wörtlich das Verfassungsgericht des Landes Brandenburg, Urteil vom 30.06.1999, VfGBbg 3/98 S. 45, im Anschluss an BVerfGE 65 S. 1ff 46; s. dazu auch unter B

Der Verdacht, dass hier in grober Weise das Recht der Betroffenen auf informationelle Selbstbestimmung missachtet worden sei, veranlasste uns, eine unangemeldete datenschutzrechtliche Prüfung des Verfahrens im Einwohnermeldeamt Potsdam durchzuführen.

Im Ergebnis der Prüfung haben wir festgestellt, dass der Verdacht sich bestätigt hat. Begünstigt durch das in Potsdam eingesetzte EDV-Programm und die unzulängliche Arbeitsorganisation sind versehentlich die Daten all jener Wahlberechtigten übermittelt worden, die zuvor dieser Übermittlung nach dem Brandenburgischen Meldegesetz widersprochen hatten.

Auch in anderen Kommunen wurden in Einzelfällen Meldedaten an die DVU übermittelt, obwohl die Bürgerinnen und Bürger einer solchen Datenweitergabe widersprochen hatten. Darüber hinaus gingen auch zahlreiche Beschwerden von Bürgerinnen und Bürgern ein, die mit der Weitergabe ihrer Anschrift an politische Parteien nicht einverstanden waren, dieser aber nicht widersprochen hatten.

Nach der geltenden Rechtslage ist es grundsätzlich zulässig, dass die Meldebehörden Wählerlisten an politische Parteien übergeben[44]. Das Brandenburgische Meldegesetz sieht vor, dass sechs Monate vor Wahlen Auskünfte über Namen, akademische Grade und gegenwärtige Anschriften von Wahlberechtigten erteilt werden können. Die entsprechenden Auskünfte an Parteien können auch nach Altersgruppen geordnet werden, wobei die Geburtstage der Wahlberechtigten nicht mitgeteilt werden dürfen. Damit lässt sich auch erklären, dass die persönlichen Anschreiben der DVU nur an eine bestimmte Altergruppe gerichtet worden sind.

Die Meldebehörde ist nicht zur Auskunftserteilung verpflichtet, sondern es besteht ein Ermessen. Nach der Rechtsprechung ist es zulässig, dass an keine Partei solche Auskünfte erteilt werden, wenn dies im Interesse des Rechts auf informationelle Selbstbestimmung der Betroffenen geboten ist. Dies ist namentlich dann der Fall, wenn eine große Zahl von Widersprüchen gegen Melderegisterauskünfte an Parteien vorliegt. Einige Kommunen, darunter eine kreisfreie Stadt, haben ihr Ermessen in dieser Art und Weise ausgeübt.

Die einzige Möglichkeit der Bürgerinnen und Bürger, etwas gegen die Weitergabe ihrer Daten an politische Parteien, an Adressbuchverlage oder anlässlich von Alters- und Ehejubiläen z. B. an die Presse zu unternehmen, ist der

---

[44] vgl. Tätigkeitsbericht 1998, 4.3

Widerspruch bei der zuständigen Meldebehörde. Dieser kann formlos erfolgen. Wir empfehlen allen Bürgerinnen und Bürgern, die eine solche Auskunft nicht wünschen, von ihrem Widerspruchsrecht Gebrauch zu machen.

Liegt ein Widerspruch vor, ist eine Weitergabe an politische Parteien - wie in der Landeshauptstadt Potsdam geschehen - unzulässig und stellt einen schweren Verstoß gegen datenschutzrechtliche Bestimmungen dar. Diesen Verstoß habe ich förmlich beanstandet. Die Stadtverwaltung hat den Vorfall zum Anlass genommen, zahlreiche organisatorische Veränderungen bei der Erteilung von Melderegisterauskünften an Parteien vorzunehmen.

So werden die Bürgerinnen und Bürger nunmehr durch ein rotes Merkblatt bei der Anmeldung auf die Widerspruchsrechte hingewiesen. Die Stadtverwaltung hat einen Vordruck für die Erklärung von Widersprüchen entwickelt. Die Bürgerinnen und Bürger erhalten das Original und das Einwohnermeldeamt eine Durchschrift. Damit ist eine ordnungsgemäße Dokumentation bei der Meldebehörde gewährleistet.

Darüber hinaus hat die Stadtverwaltung eine Dienstanweisung für die Bearbeitung von Gruppenauskünften (dazu gehören auch die Auskünfte an Parteien) und Datenübermittlungen aus dem Melderegister in Kraft gesetzt, die eine datenschutzgerechte Bearbeitung sicherstellt. Dem Beispiel Potsdams sollten auch die anderen Meldebehörden in Brandenburg folgen und Maßnahmen zur Unterstützung und Umsetzung der Widerspruchsrechte der Betroffenen ergreifen.

Nach der neu erlassenen Verordnung zur Durchführung des Gesetzes über das Meldewesen im Land Brandenburg sind nunmehr Meldescheine bei der Anmeldung verbindlich, auf denen Felder für die Eintragung von Widersprüchen gegen bestimmte Melderegisterauskünfte vorgesehen sind. Dies begrüßen wir.

Die Vielzahl der Beschwerden zeigt, dass die Widerspruchslösung aus datenschutzrechtlicher Sicht nicht zufriedenstellen kann. Wie bereits in unserem Tätigkeitsbericht 1998 ausgeführt, ist eine Änderung des Meldegesetzes dringend geboten. Auskünfte aus dem Melderegister an Parteien oder Adressbuchverlage, aber auch anlässlich von Alters- oder Ehejubiläen sollten nur noch dann zulässig sein, wenn die Bürgerinnen und Bürger ausdrücklich eingewilligt haben.

Die Widerspruchslösung bei Melderegisterauskünften an politische Parteien, Adressbuchverlage sowie anlässlich von Alters- und Ehejubiläen berücksichtigt nicht in ausreichendem Maße das Recht auf informationelle

Selbstbestimmung der Bürgerinnen und Bürger. Solche Auskünfte sollten ausschließlich von der vorherigen Einwilligung der Betroffenen abhängig gemacht werden.

4.3.2 Zwei Melderegister in einer Gemeinde?

Eine amtsfreie Gemeinde wandte sich mit folgendem Problem an uns:

Meldestelle und Kämmerei befinden sich in verschiedenen, mehrere Kilometer auseinander liegenden, Ortsteilen der Gemeinde. Die Kämmerei benötigt für die Versendung von Steuer- und Vollstreckungsbescheiden die Anschriften der Schuldner. Eine Reihe von Bescheiden sei nicht ordnungsgemäß zustellbar, weil die aktuellen Anschriften nicht bekannt seien. Die Gemeinde beabsichtigte daher, eine ständig aktualisierte Kopie der kompletten Meldedatei in dem Ortsteil bereitzuhalten, in dem sich die Kämmerei befand.

Nach dem Brandenburgischen Meldegesetz sind Meldebehörden u. a. die amtsfreien Gemeinden als örtliche Ordnungsbehörden. Daraus folgt jedoch nicht, dass die Meldedatei von verschiedenen Ämtern innerhalb der Gemeindeverwaltung gespeichert werden kann. Zwar ist nach dem Grundsatz der Einheit der Kommunalverwaltung die Gemeinde insgesamt als Daten verarbeitende Stelle im Sinne des Datenschutzrechts anzusehen. Aus dem zentralen datenschutzrechtlichen Grundsatz, dass personenbezogene Daten in der Regel nur zu Zwecken verarbeitet werden dürfen, für die sie erhoben worden sind, folgt jedoch, dass auch innerhalb einer öffentlichen Stelle bei der Datenverarbeitung eine Trennung nach Aufgabenbereichen erfolgen muss. Dieser vom Bundesverfassungsgericht aufgestellte Grundsatz der informationellen Gewaltenteilung hat seinen Ausdruck u. a. auch in der neuen Vorschrift des § 28 Abs. 4 Brandenburgisches Meldegesetz (BbgMeldeG) gefunden. Danach ist die Weitergabe von Meldedaten innerhalb der Gemeinde einer Datenübermittlung gleichgestellt. Aus diesem Grunde ist es nicht möglich, außerhalb der Meldebehörde eine zweite Ausfertigung der Meldedatei zu speichern.

Aus dem gleichen Grunde sehen wir keine Möglichkeit, dass die Meldebehörde die Anschriften aller Gemeindeeinwohner an andere Ämter der Gemeinde, beispielsweise die Kämmerei, weitergibt. Zwar ist es nach dem Brandenburgischen Meldegesetz ohne Weiteres möglich, Namen und Anschriften von Einwohnern aus dem Melderegister an andere Ämter innerhalb der Gemeinde zu übermitteln. § 28 Abs. 4 BbgMeldeG lässt dies allerdings nur unter den Voraussetzungen des § 28 Abs. 1 BbgMeldeG zu. Dies bedeutet, dass die Daten nur dann weitergegeben werden dürfen, wenn dies zur Aufgabenerfüllung insbesondere des Empfängers, also beispielsweise

der Kämmerei, erforderlich ist. Die Kämmerei benötigt aber lediglich die Anschriften der Steuerpflichtigen und Vollstreckungsschuldner der Gemeinde. Der Empfänger der Daten würde also mehr Informationen erhalten, als er zur Aufgabenerfüllung benötigt, wenn er die komplette Einwohnerdatei zur Verfügung gestellt bekäme.

Ebenfalls ist es nicht möglich, dass die Kämmerei bei der Meldebehörde nur die Anschriften der steuerpflichtigen Bürgerinnen und Bürger anfordert. Damit würde offenbar werden, welche Einwohner der Gemeinde steuerpflichtig sind, auch wenn noch nicht feststeht, für welche Art von Steuern dies der Fall ist. Bereits die Angabe, dass jemand steuerpflichtig ist, fällt unter das Steuergeheimnis nach § 30 Abgabenordnung (AO). Eine Offenbarungsbefugnis nach § 30 Abs. 4 AO ist nicht vorhanden.

Schließlich wäre auch eine regelmäßige Datenweitergabe, der ein automatisierter Abruf gleichgestellt ist, unzulässig. Nach unserer Auffassung müssen auch bei der Weitergabe von Meldedaten innerhalb einer Gemeinde die Voraussetzungen des § 29 BbgMeldeG für regelmäßige Datenübermittlungen erfüllt sein. Es existiert aber keine Rechtsvorschrift, die dies zulässt. Insbesondere ergibt sich aus der aufgrund § 29 Abs. 2 BbgMeldeG erlassenen Meldedatenübermittlungsverordnung keine Übermittlungsbefugnis. Dies ist aus unserer Sicht auch sachgerecht, weil es kein Bedürfnis für eine solche regelmäßige Datenweitergabe gibt. Im Unterschied beispielsweise zu den Finanzämtern benötigen die kommunalen Steuerämter regelmäßig nur die Daten eines Teils der Gemeindeeinwohnerinnen und -einwohner.

Zulässig ist es aus unserer Sicht, wenn die Kämmerei Daten nur derjenigen Gemeindeeinwohnerinnen und -einwohner anfordert, bei denen sich die Bescheide wegen falscher Anschrift nicht zustellen ließen.

Wir haben die Gemeinde außerdem darauf hingewiesen, dass Steuerpflichtige nach der Abgabenordnung selbst verpflichtet sind, die erforderlichen Auskünfte für das Besteuerungsverfahren zu erteilen, darunter die neue Anschrift nach einem Umzug. Kommen die Steuerpflichtigen der Auskunftspflicht nicht nach, so ist im Einzelfall eine Weitergabe von Meldedaten unter den Voraussetzungen von § 28 Abs. 4 BbgMeldeG ohne Weiteres zulässig. Es wäre zu überlegen, ob die durch solche Ermittlungen entstehenden Mehrkosten nicht von den Steuerpflichtigen zu tragen sind, da diese ihrer Auskunftspflicht nach der Abgabenordnung nicht nachgekommen sind.

Die Führung von zwei Melderegistern innerhalb des Trägers einer Meldebehörde ist nicht zulässig. Die regelmäßige Weitergabe von Daten aus dem Melderegister innerhalb des Trägers der Meldebehörde ist nur unter den Voraussetzungen zulässig, die auch für regelmäßige Meldedatenübermittlungen an andere Stellen gelten.

4.4 Personaldaten

4.4.1 Bewerbungsunterlagen in der Justiz

Wie in allen anderen Bundesländern gelten auch in Brandenburg die bundeseinheitlichen "Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden", die durch Verfügung des Ministers der Justiz und für Europaangelegenheiten in Kraft gesetzt werden. Sie sind damit verbindlich für alle ordentlichen Gerichte, die Staatsanwaltschaften und die Justizvollzugsanstalten des Landes. Diese Aufbewahrungsbestimmungen enthalten nicht nur Regeln zur Aufbewahrung von Justizakten, sondern auch von Personalakten der in der Justiz beschäftigten Personen. So ist u. a. festgelegt, dass Bewerbungsvorgänge, die nicht in Personalakten einmünden, fünf Jahre aufzubewahren sind. Dies bedeutet, dass Unterlagen von abgelehnten Bewerberinnen und Bewerbern für diesen Zeitraum aufbewahrt werden müssten und eigentlich auch nicht an sie zurückgesendet werden könnten.

Diese Bestimmung ist aus unserer Sicht nicht haltbar. Da spezielle Vorschriften für die Personaldatenverarbeitung im Bereich der Justiz nicht existieren, müssen sich die Aufbewahrungsbestimmungen im Rahmen dessen bewegen, was nach § 29 BbgDSG zulässig ist. Nach dieser Vorschrift sind personenbezogene Daten, die vor Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben werden, unverzüglich zu löschen, sobald feststeht, dass ein Beschäftigungsverhältnis nicht zu Stande kommt. Eine weitergehende Speicherung solcher Unterlagen wäre nur zulässig, wenn die Betroffenen darin einwilligen.

Vor diesem Hintergrund sind die oben zitierten Aufbewahrungsfristen eindeutig zu lang. Sobald feststeht, dass eine Bewerberin oder ein Bewerber nicht eingestellt wird, sollten daher - wie allgemein üblich - die Bewerbungsunterlagen unverzüglich zurückgegeben werden.

Die Bewerbungsschreiben selbst können für einen gewissen Zeitraum nach Abschluss des Bewerbungsverfahrens aufbewahrt werden. Dies ist beispielsweise aus Gründen der Dokumentation oder wegen gelegentlicher Rückfragen erforderlich. Dieser Zeitraum sollte aber nicht mehr als ein Jahr umfassen.

Das Ministerium der Justiz und für Europaangelegenheiten teilt unsere Auffassung und hält die Aufbewahrungsfristen ebenfalls für zu lang. Es hat deshalb die Justizministerien der übrigen Bundesländer um ihre Meinung gebeten und will sich gegebenenfalls für eine Änderung der bundeseinheitlichen Bestimmungen einsetzen.

Bewerbungsunterlagen sind unverzüglich nach Abschluss des Bewerbungsverfahrens zurückzusenden. Anschreiben zur Bewerbung können für einen gewissen Zeitraum - etwa ein Jahr - aufbewahrt werden. Von diesen Grundsätzen kann nur dann abgewichen werden, wenn die betroffene Person einwilligt.

4.4.2 Organisationsuntersuchungen des Landesrechnungshofs

Ein Ministerium hat uns davon in Kenntnis gesetzt, dass der Landesrechnungshof bei einer nachgeordneten Landesoberbehörde sowie den dazugehörenden unteren Landesbehörden eine Untersuchung der Organisation und des Personalbedarfs durchführt. Zu diesem Zweck überreichten Beauftragte des Landesrechnungshofs den Bediensteten der Verwaltung jeweils einen Fragebogen mit einem Begleitschreiben. Die Beschäftigten wurden gebeten, namentlich gekennzeichnete Fragebögen auszufüllen und Fragen zu Weisungssträngen, Arbeitsabläufen, Informationsflüssen, häufig auftretenden Störungen und zum Arbeitsklima zu beantworten und Lösungs- und Verbesserungsvorschläge zu machen. Das Begleitschreiben enthielt einige allgemeine Informationen zum Zweck der Untersuchung. Ziel der Befragung war danach, allgemeine Informationen zur Aufgabenwahrnehmung zu erhalten und die häufigsten Störungen kennen zu lernen, um letztlich die Organisation allgemein zu verbessern. Im Übrigen wurde Vertraulichkeit zugesichert und ausgeführt, dass die Antworten nach Sachgruppen zusammengefasst werden, um direkte Rückschlüsse auf einzelne Beschäftigte auszuschließen.

Das Ministerium bat uns, den Fragebogen sowie das Begleitschreiben aus datenschutzrechtlicher Sicht zu bewerten.

Der Landesrechnungshof ist nach der Brandenburgischen Landesverfassung eine selbständige, unabhängige oberste Landesbehörde. Seine Mitglieder genießen richterliche Unabhängigkeit. Gleichwohl ist der Landesrechnungshof, ebenso wie andere öffentliche Stellen, an Recht und Gesetz und somit auch an das materielle Datenschutzrecht des Landes Brandenburg gebunden. Soweit also keine besonderen Rechtsvorschriften existieren, gilt auch für den Landesrechnungshof das Brandenburgische Datenschutzgesetz. Besondere Vorschriften, die dem Datenschutzgesetz vorgehen, sind in diesem Sinne vor allem die Landeshaushaltsordnung (LHO) sowie das Landesrechnungshofgesetz

(LRHG). Soweit es um die Verarbeitung personenbezogener Daten bei der Rechnungsprüfung geht, gelten vor allem die Regelungen der §§ 88 ff. LHO. Soweit diese Vorschriften den Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil[45] an bereichsspezifische Gesetze zum Datenschutz gestellt hat, nicht genügen, finden ergänzend die Vorschriften des Brandenburgischen Datenschutzgesetzes auch auf die Rechnungsprüfungstätigkeit des Landesrechnungshofs Anwendung.

Nach § 95 LHO bestimmt der Landesrechnungshof selbst, welche Unterlagen er zur Erfüllung seiner Aufgaben für erforderlich hält und welche Auskünfte ihm dementsprechend zu erteilen sind. Dies bedeutet vor allem, dass die Behörde, die die Unterlagen vorlegen soll, nicht befugt ist, deren Vorlage zu verweigern. Dies gilt selbst dann, wenn sie der Auffassung ist, die Unterlagen seien für die Aufgabenerfüllung des Landesrechnungshofs nicht erforderlich. Eine andere Auslegung würde nach unserer Auffassung der Unabhängigkeit des Landesrechnungshofs widersprechen.

Im konkreten Fall hatten wir Zweifel, ob Fragebogen und Anschreiben in der oben beschriebenen Form den gesetzlichen Vorgaben entsprechen. Zunächst war für uns nicht zu erkennen, aus welchem Grund der Fragebogen mit dem Namen der Beschäftigten versehen, also personenbezogen ausgefüllt werden sollte. Der Landesrechnungshof hatte in seinem Begleitschreiben selbst ausgeführt, dass für die Auswertung der Antworten ein Personenbezug nicht erforderlich sei. Wie bei Organisationsuntersuchungen durch die Dienstbehörde ist auch hier ein Personenbezug in aller Regel nicht nötig, geht es doch in beiden Fällen um das Ziel, den Personaleinsatz zu optimieren und effektiver zu gestalten. Dafür ist es regelmäßig nicht relevant, wer eine bestimmte Stelle innehat. Es sollte daher von vornherein auf die Erhebung des Namens verzichtet werden. Dies galt hier um so mehr, als den Beschäftigten sehr persönliche und sensible Fragen, beispielsweise zum Betriebsklima gestellt wurden. Auch wenn auf die Angabe des Namens verzichtet wird, sind die Angaben aufgrund der konkreten Fragen in der Regel immer noch personenbeziehbar. Deshalb sind bei der Auswertung in jedem Fall die Antworten so früh wie möglich zu größeren Gruppen zusammenzufassen (aggregieren). Dabei ist der Grundsatz zu beachten, dass die Daten um so stärker aggregiert werden müssen, je mehr Personen im Rahmen der Auswertung davon Kenntnis erlangen.

Auch das Begleitschreiben genügte den datenschutzrechtlichen Anforderungen nicht. Dies betraf insbesondere die Aufklärungspflicht nach dem BbgDSG, die mangels spezieller Regelungen in der LHO auch bei der Tätigkeit des Landesrechnungshofs zu beachten ist. Die Beschäftigten sind danach umfassend und detailliert darüber aufzuklären,

[45] BVerfGE 65, 1 ff.

in welcher Art und Weise mit den von ihnen erlangten Informationen umgegangen werden soll. Hält der Landesrechnungshof nach dem oben Gesagten die Angaben für die Erfüllung seiner Aufgaben für erforderlich, so sind die Beschäftigten ausdrücklich auf die Auskunftspflicht nach der LHO hinzuweisen. Ist dies nicht der Fall, so müssen die Beschäftigten darauf hingewiesen werden, dass die Angaben freiwillig sind.

Wir haben dem Landesrechnungshof unsere Bedenken mitgeteilt und ihn gebeten, unsere Empfehlungen zu berücksichtigen.

Der Landesrechnungshof hat daraufhin sowohl den Fragebogen als auch das Begleitschreiben überarbeitet. Nunmehr wurde auf die Angabe des Namens von vornherein verzichtet. Im Begleitschreiben wurde ausdrücklich darauf hingewiesen, dass das Ausfüllen des Fragebogens freiwillig geschieht.

Für die Tätigkeit des Landesrechnungshofs gelten trotz seiner besonderen verfassungsrechtlichen Stellung die Bestimmungen des materiellen Datenschutzrechts. Der Landesrechnungshof bestimmt allerdings aufgrund seiner Unabhängigkeit selbst, welche Informationen er im Rahmen seiner Prüftätigkeit benötigt. Organisationsuntersuchungen sollten auch vom Landesrechnungshof so durchgeführt werden, dass möglichst von vornherein auf einen direkten Personenbezug verzichtet wird. Die Daten sind so früh wie möglich zu größeren Gruppen zusammenzufassen.

4.4.3 Besoldungsmitteilungen auf dem Kontoauszug

Eine Beamtin des Landes Brandenburg beschwerte sich darüber, dass sie auf ihren Kontoauszügen wiederholt Mitteilungen vorfand, die bestimmte Modalitäten ihrer Besoldung betrafen. Insbesondere war bei der Überweisung der Besoldung im Feld "Verwendungszweck" angegeben, dass die Zahlungen vorläufig erfolgten. Diese Informationen waren somit auch der Konto führenden Bank zugänglich.

Die Weitergabe bestimmter Informationen über die Modalitäten der Besoldung stellt datenschutzrechtlich gesehen eine Übermittlung personenbezogener Daten an die Konto führende Bank dar. Dafür gibt es allerdings keine Rechtsgrundlage. Je nachdem, ob die Konto führende Bank ein öffentlich-rechtlich organisiertes (Sparkasse) oder ein privates Kreditinstitut ist, handelt es sich entweder um eine Datenübermittlung innerhalb des öffentlichen Bereichs oder um eine solche an Personen oder Stellen außerhalb des öffentlichen Bereichs. Zwar ist die Zulässigkeit solcher Datenübermittlungen in beiden Fällen nach unterschiedlichen Rechtsvorschriften des Brandenburgischen Datenschutzgesetzes zu beurteilen. Alle diese Vorschriften setzen jedoch voraus, dass die Daten zur Erfüllung der

Aufgaben der übermittelnden oder der empfangenden Stelle erforderlich sind und nur zu dem Zweck übermittelt werden dürfen, zu dem sie auch erhoben worden sind. Diese Voraussetzungen sind hier nicht erfüllt. Die Konto führende Bank benötigt die in Rede stehenden Informationen nicht, um den mit dem Zahlungsvorgang angewiesenen Betrag auf dem Konto der Beamtin gutzuschreiben. Eine Nutzung zu anderen Zwecken, beispielsweise um den Kreditrahmen festzulegen, ist jedenfalls unzulässig.

Die Zentrale Bezügestelle des Landes Brandenburg hat dieses Verfahren aus Gründen der Praktikabilität gewählt. Da die Beamtinnen und Beamten nicht jeden Monat eine Besoldungsmitteilung erhielten, werde der Weg über den Kontoauszug gewählt, um ihnen wichtige Tatsachen mitzuteilen.

Wir haben die Zentrale Bezügestelle darauf hingewiesen, dass diese Datenübermittlung nicht zulässig ist und sie gebeten, in Zukunft ein anderes, datenschutzgerechtes Verfahren für solche Mitteilungen zu wählen.

4.4.4 Gehört ein Arbeitsgerichtsurteil in die Personalakte?

Ein Angestellter der Finanzverwaltung beschwerte sich, dass seine Personalakte Unterlagen enthalten würde, die nach seiner Auffassung nicht in der Personalakte hätten abgelegt werden dürfen. Er gab an, dass die Personalakte u. a. ein vollständiges Urteil aus einem Kündigungsrechtsstreit beim Arbeitsgericht, einen Vermerk der Oberfinanzdirektion über eine Anhörung wegen verschiedener arbeitsrechtlicher Verstöße sowie verschiedene Unterlagen über seine Angehörigen aus dem Arbeitsgerichtsverfahren enthielt. Er sah sich und seine Angehörigen dadurch in den Persönlichkeitsrechten verletzt.

Wir haben die Oberfinanzdirektion gebeten, den Inhalt der Personalakte zu prüfen und zum Sachverhalt Stellung zu nehmen. Dabei haben wir die Oberfinanzdirektion darauf hingewiesen, dass auch für die Führung von Personalakten der Angestellten die Aussagen des Landesbeamtengesetzes zu Grunde zu legen sind. Demnach dürfen Personalakten nur Unterlagen enthalten, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen. Deshalb gehören sämtliche Unterlagen über arbeitsrechtliche Ermittlungen einschließlich der Urteilsbegründung des Arbeitsgerichts in die bei der Rechtsabteilung geführten Prozessakten. Lediglich der Tenor des Arbeitsgerichtsurteils kann in der Personalakte gespeichert werden.

Die Oberfinanzdirektion hat daraufhin den Inhalt der Personalakte geprüft und konnte feststellen, dass die Personalakte das Urteil des Arbeitsgerichts und den Vermerk der Oberfinanzdirektion tatsächlich enthielt. Die übrigen Unterlagen befanden sich hingegen nicht in der Personalakte.

Die Oberfinanzdirektion ist unseren Empfehlungen unverzüglich gefolgt und hat sowohl den Vermerk als auch das Urteil mit Ausnahme des Tenors aus der Personalakte entfernen lassen.

Für das Führen von Personalakten der Angestellten werden die Vorschriften des Landesbeamtengesetzes entsprechend angewendet. Personalakten dürfen nur Unterlagen enthalten, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen. Unterlagen über arbeitsrechtliche oder disziplinarische Ermittlungen müssen getrennt von der Personalakte aufbewahrt werden.

4.4.5 Wer darf in personenbezogene Unterlagen des Personalrats einsehen?

Der Personalrat einer Stadtverwaltung wandte sich an uns, weil der Bürgermeister die Herausgabe eines bestimmten Sitzungsprotokolls oder Beschlusses des Personalrats verlangte und auch ein Schreiben, in dem der Personalrat einige Beschäftigte der Verwaltung zu Beratungsgesprächen eingeladen hatte, um sie auf eine geplante Teilzeitbeschäftigung vorzubereiten. Die Sorge des Personalrats bestand darin, dass er bei der Herausgabe der gewünschten Unterlagen, die z. T. auch personenbezogene Beschäftigtendaten enthielten, datenschutz- und personalvertretungsrechtliche Verstöße begehen würde. Der Bürgermeister wiederum bestritt dem Personalrat das Recht, sich unmittelbar an uns zu wenden.

Der Personalrat hatte Recht, bei der Herausgabe seiner eigenen Unterlagen an den Bürgermeister zu zögern. Denn die Sitzungen des Personalrats sind nach § 10 des Brandenburgischen Personalvertretungsgesetzes (PersVG) nicht öffentlich. Daraus folgt, dass die Sitzungsprotokolle wie auch die Willensbildung des Personalrats nicht öffentlich sind. Ein gesetzlicher oder sonstiger Anspruch der Dienststellenleitung auf Herausgabe von Unterlagen des Personalrats besteht grundsätzlich nicht. Ein solcher Anspruch besteht nur für den - hier nicht gegebenen - Fall, dass ein Vertreter der Dienststellenleitung an der Sitzung des Personalrats teilgenommen hat, und dann auch nur für die Tagesordnungspunkte, die während seiner Anwesenheit behandelt wurden.

Allerdings haben sowohl Dienststellenleitung als auch die übrigen Beschäftigten ein Recht darauf, über Folgen von Beratungen und Beschlüssen des Personalrats informiert zu werden, wenn sie selbst in irgendeiner Weise betroffen

sind. Diese Unterrichtung war aber in unserem Fall längst zu Stande gekommen, und zwar sogar in einer förmlichen und protokollierten Erklärung des Personalrats.

Die Herausgabe von Schreiben des Personalrats, die er an betroffene Beschäftigte gerichtet hatte, oder die Weitergabe von Inhalten der mit den betroffenen Beschäftigten geführten Gespräche an die Dienststellenleitung ist dagegen unzulässig, weil diese Daten ausdrücklich der Schweigepflicht nach § 10 PersVG unterliegen.

Zu Unrecht war der Bürgermeister auch der Meinung, der Personalrat oder einzelne seiner Mitglieder dürften sich nicht unmittelbar an den Landesbeauftragten wenden. Das Personalvertretungsgesetz sieht dieses Anrufungsrecht für Personalräte ausdrücklich vor (§ 94 Abs. 2 PersVG). Auch sonstige Beschäftigte im öffentlichen Dienst haben das Recht, sich ohne Einhaltung des Dienstweges an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu wenden, wenn sie sich in ihrem Recht verletzt sehen. Sie dürfen deshalb weder benachteiligt noch gemaßregelt werden (§ 21 BbgDSG).

Unterlagen, Protokolle und personenbezogene Daten des Personalrats müssen nicht an die Dienststellenleitung herausgegeben werden. Personalräte und Beschäftigte können sich unmittelbar an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht wenden, ohne dafür benachteiligt oder gemaßregelt zu werden.

4.4.6 Namensschilder an Bürotüren

Der behördliche Datenschutzbeauftragte eines Landkreises informierte uns darüber, dass die Kreisverwaltung in ein neues Dienstgebäude umziehe. Der Landrat wünschte, dass an allen Bürotüren der Beschäftigten in der Kreisverwaltung Namensschilder mit den vollständigen Namen - also Vor- und Nachnamen - angebracht werden.

Einige Beschäftigte, die vor allem in sensiblen Bereichen wie Jugendamt oder Sozialamt tätig sind, wünschten jedoch nicht, dass ihr Vorname an der Tür erscheint. Da die Flure für den Publikumsverkehr zugänglich sind, befürchteten sie, damit auch in ihrem privaten Umfeld leichter identifizierbar zu sein. Der behördliche Datenschutzbeauftragte bat uns, unsere Rechtsauffassung darzulegen.

Entscheidend für die Frage, inwieweit es die Bediensteten hinnehmen müssen, dass Namensschilder mit Vor- und Familiennamen an den Bürotüren angebracht werden, ist, in welchem Umfang sich Beschäftigte im öffentlichen Dienst - also Amtsträger - auf das Recht auf informationelle Selbstbestimmung berufen können.

Auch in ihrer Eigenschaft als Amtsträger bleibt eine Person Trägerin von Grundrechten. Sie muss es aber hinnehmen, dass ihre Rechte eingeschränkt werden können, soweit es zur Durchführung ihrer dienstlichen Tätigkeit geboten ist.

Aus der Fürsorgepflicht des Dienstherrn gegenüber den Beschäftigten folgt, dass bestimmte Informationen über die Amtsträger nicht preisgegeben werden dürfen.

Danach bestehen im Allgemeinen keine Bedenken, wenn der Familienname des Amtsträgers an den Bürotüren erscheint, soweit es sich nicht um besonders gefährdete Personen (z. B. wegen einer exponierten Tätigkeit) handelt. Damit ist das berechtigte Informationsinteresse der Bürgerinnen und Bürger aber auch gedeckt.

Hinsichtlich der Vornamen der Bediensteten besteht jedoch kein überwiegendes Informationsinteresse der Bürgerinnen und Bürger. Für die Tätigkeit nach außen ist es ausreichend, dass die Bürger die Person des Bediensteten identifizieren können und das Geschlecht erkennbar ist. Der Vorname ist dafür grundsätzlich nicht erforderlich.

Öffentlich Bedienstete müssen in ihrer Eigenschaft als Amtsträger Einschränkungen ihres Rechts auf informationelle Selbstbestimmung nur hinnehmen, soweit dies zur Erfüllung ihrer dienstlichen Aufgaben erforderlich ist. Die Beschäftigten müssen aber die Nennung ihres Vornamens an der Bürotür nicht hinnehmen.

4.5 Statistik

4.5.1 Neues von der Hochbaustatistik

Seit Beginn des Jahres 1999 gilt in Deutschland ein neues Hochbaustatistikgesetz[46]. Hiernach werden dem Bauherren Angaben über die Baugenehmigung, die Baufertigstellung, den Bauüberhang und den Bauabgang abverlangt.

Aufgrund von Hinweisen anderer Landesdatenschutzbeauftragter haben wir geprüft, wie dieses Gesetz im Land Brandenburg umgesetzt wird. Wie in den anderen Bundesländern wird dem auskunftspflichtigen Bauherren ein Erhebungsbogen ausgehändigt, den er ausfüllen muss. Diesen Bogen gibt der Bauherr bei der zuständigen Bauaufsichtsbehörde ab, die ihrerseits dessen Angaben überprüft, bestätigt und an das Brandenburgische Landesamt für Datenverarbeitung und Statistik weiterreicht.

Dies ist zwar ein recht einfaches und praktisches Verfahren; es verstößt jedoch gegen das Prinzip der Trennung von Statistik und Verwaltungsvollzug. Denn nach den Statistikgesetzen sind Auskunftspflichtige nur zur statistischen Auskunft gegenüber amtlichen Stellen und Personen verpflichtet, die mit der Durchführung der Statistik betraut sind. Dies sind Statistikstellen und das Landesamt für Datenverarbeitung und Statistik, nicht jedoch Gemeinden, Ämter oder Bauaufsichtsbehörden.

Um zu einer praktikablen Lösung zu kommen, haben wir vorgeschlagen, dass die zuständigen Bauaufsichtsbehörden generell allein die statistischen Daten als Sekundärstatistik an das Landesamt für Datenverarbeitung und Statistik liefern; der Bauherr sollte lediglich über dieses Verfahren unterrichtet werden.

In Gesprächen mit dem Innenministerium und anderen zuständigen Behörden wurde allerdings deutlich, dass das Datenmaterial der Baubehörden nicht ausreichend ist. Dies betrifft etwa Daten zu Wohnungsunternehmen, Immobilienfonds, zu Unternehmen der Land- und Forstwirtschaft, des Handels, der Kreditinstitute usw.

Da dieses Problem jedoch alle Bundesländer angeht, sollte auch nach einer gemeinsamen Lösung gesucht werden.

In den Bundesländern ist das jetzige Verfahren der Datenerhebung zur Hochbaustatistik datenschutz- und statistikrechtlich unzulässig. Dazu muss ein neues Erhebungsverfahren entwickelt werden. Möglich ist zz. nur die Lieferung von Sekundärstatistiken durch die Bauaufsichtsbehörden.

4.5.2 Prüfung kommunaler Statistikstellen

[46] Gesetz über die Statistik der Bautätigkeit im Hochbau und die Fortschreibung des Wohnungsbestandes vom 5. 5.1998, BGBl. I S. 869.

Seit 1996 ist das Brandenburgische Statistikgesetz in Kraft. Danach sind kommunale Statistikstellen befugt, für statistische Zwecke Einzelangaben aus Statistiken der EU und aus Bundes- und Landesstatistiken vom Landesamt für Datenverarbeitung und Statistik zu erhalten, sofern sie in einer besonderen Dienstanweisung schriftlich nachgewiesen haben, dass sie die zur Gewährleistung der statistischen Geheimhaltung erforderlichen Regelungen verbindlich festgelegt haben. Zur Unterstützung der Kommunen und der Kommunalverbände hatte das Innenministerium eine Muster-Dienstanweisung zur Aufgabenbeschreibung und Abschottung der kommunalen Statistikstelle vorgelegt.

Neben den o. g. Aufgaben führen kommunale Statistikstellen Primärerhebungen für eigene Statistiken und Geschäftsstatistiken für andere Verwaltungsstellen als Datenverarbeitung im Auftrag durch. Auch sind sie Erhebungsstellen für EU-, Bundes- und Landesstatistiken.

Als Statistikstellen müssen sie räumlich, organisatorisch, technisch und personell von den anderen Stellen des Verwaltungsvollzugs abgeschottet sein. Es gilt nämlich, ein grundsätzliches Vertrauen der Bevölkerung in die Wahrung des Statistikgeheimnisses aufzubauen und zu erhalten. Dazu muss in den kommunalen Statistikstellen eine ständige und dauerhafte rechentechnische „Vertrauens"-Infrastruktur vorhanden sein, die es jederzeit ermöglicht, dass Einzeldatensätze abgeschottet verarbeitet werden können. Nicht einmal zehn Statistikstellen haben derzeit im Land Brandenburg einen ausreichenden Abschottungsstandard.

Prüfungsziel war es, bei mehreren Statistikstellen die technisch-organisatorischen Maßnahmen und insbesondere die Abschottung der Computer der Statistikstelle von der übrigen Verwaltung anhand der Dienstanweisung zu kontrollieren.

Die Muster-Dienstanweisung zur Aufgabenbeschreibung und Abschottung der kommunalen Statistikstelle geht von zwei Varianten des Computereinsatzes aus: Entweder betreibt eine Statistikstelle ihre Rechner nur lokal und damit physikalisch getrennt vom übrigen Verwaltungsnetz, oder aber sie setzt zwingend eine sog. starke kryptographische Verschlüsselung für die Leitungsübertragung und für die Speicherung der statistischen Daten ein. Unter diesen Bedingungen wäre die Nutzung des allgemeinen Behördennetzes möglich. Auch ist es nach der Muster-Dienstanweisung vorgesehen, dass die Statistikstelle mit einem speziellen Rechner mit dem Behördennetz verbunden sein kann.

Die geprüften Statistikstellen verfügten meistens über lokale Rechner. In einem Fall wurde festgestellt, dass die Computer der Statistikstelle entgegen der eigenen Dienstanweisung komplett in das Behördennetz integriert waren, ohne dass eine entsprechende Verschlüsselungssoftware genutzt wurde. Allerdings hatte man hier bisher noch keine personenbezogenen Einzelangaben automatisiert verarbeitet und gespeichert.

Eine weitere zulässige Variante der Computernutzung in der Statistikstelle wäre beispielsweise, nur einen Rechner lokal und physikalisch getrennt vom übrigen Behördennetz zu betreiben und für die Einzelangabenverarbeitung zu nutzen. Die übrigen Rechner der Statistikstelle könnten dann mit dem Behördennetz dauerhaft verbunden sein, wenn garantiert ist, dass die auf dem zentralen Server gespeicherten statistischen Daten zuvor auf dem Einzelplatz der Statistikstelle so stark anonymisiert und aggregiert worden sind, dass der Rückschluss auf eine bestimmte Person mit Sicherheit ausgeschlossen werden kann.

Bei unserer Prüfung der Statistikstellen haben wir auch erfahren, dass Stadtverwaltungen häufig statistische Primärerhebungen wie Bürgerbefragungen, Wohnumfeldanalysen, Verkehrsbefragungen u. Ä. durchführen. Hierbei müssen allerdings zukünftig verstärkt die Anforderungen des Brandenburgischen Statistikgesetzes über die Vergabe statistischer Arbeiten berücksichtigt werden. Selbst wenn die Erhebungen anonym erfolgen, können beispielsweise Interviewer während der Befragung personenbezogenes Zusatzwissen etwa über das Wohnumfeld oder über die soziale Lage der Befragten erlangen. Dieses Zusatzwissen muss durch besondere Geheimhaltungsmaßnahmen geschützt werden.

Auch ist zu beachten, dass bei der Vergabe statistischer Arbeiten an nicht-öffentliche Stellen wie etwa Vereine oder ABM-Kräfte diese sich der Kontrolle des öffentlichen Auftraggebers unterwerfen müssen.

Generell ist bei einer Auftragsvergabe sicherzustellen, dass beim Auftragnehmer die Vorschriften zum Schutz personenbezogener Daten und der statistischen Geheimhaltung eingehalten und dass entsprechende Verträge über die Datenverarbeitung im Auftrag abgeschlossen werden.

Sowohl in der Muster-Dienstanweisung zur Aufgabenbeschreibung und Abschottung der kommunalen Statistikstelle als auch in den entsprechenden örtlichen Dienstanweisungen wird die besondere Rolle der Statistikstelle bei der Beratung anderer Verwaltungsstellen dargestellt. Dies gilt auch für die Beteiligung der Statistikstelle bei der Vergabe statistischer Arbeiten an öffentliche und private Auftragnehmer.

Hier muss jedoch der Informationsfluss innerhalb der Kommunen offensichtlich noch verbessert werden. Denn oft erfährt eine Statistikstelle erst im Nachhinein oder zufällig von statistischen Erhebungen, die von anderen Stellen der eigenen Verwaltung vergeben worden sind. Die Statistikstelle muss jedoch über alle statistischen Vorhaben der Stadtverwaltung rechtzeitig informiert werden, um ihren Beratungsauftrag erfüllen zu können.

Nur eine gut ausgerüstete, sicher abgeschottete und gut informierte Statistikstelle ist in der Lage, eine vertrauenswürdige Infrastruktur aufzubauen und zu erhalten und das Vertrauen der Bevölkerung in die Durchführung von Statistiken zu festigen.

4.6 Kommunalrecht

4.6.1 Datenschutz und Kommunalverfassung - was müssen und dürfen die Gemeindevertreter wissen?[47]

Häufig erreichten uns Anfragen aus den Kommunen sowohl von Gemeindevertretern oder Stadtverordneten als auch von den Kommunalverwaltungen, die den Umfang von Auskunftsrechten der Gemeindevertretungen oder Stadtverordnetenversammlungen gegenüber Bürgermeister oder Amtsdirektor betreffen. Die Bürgermeister (Amtsdirektoren) sind dabei oft unsicher, welche Informationen sie den Kommunalvertretungen zur Verfügung stellen müssen und welche Auskünfte sie nicht erteilen dürfen.

So wurde uns beispielsweise vom Bürgermeister einer amtsfreien Stadt eine Beschlussvorlage einer in der Stadtverordnetenversammlung vertretenen Fraktion zur Prüfung vorgelegt, in der die Vorlage einer Grundstücksliste begehrt wurde. Die Liste sollte zum einen alle städtischen Grundstücke enthalten und solche, bei denen Verkaufsverhandlungen geführt wurden bzw. beabsichtigt sind. Zum anderen sollte aber auch kenntlich gemacht werden, wer Eigentümer von Grundstücken mit mehr als 2.500 m² bzw. von mehr als zwei Grundstücken in der Gemarkung ist.

In einer anderen amtsfreien Gemeinde ist auf Antrag von zwei Fraktionen der Gemeindevertretung beschlossen worden, dass der Bürgermeister eine Grundstücksliste zu übergeben habe. Aus dieser sollte sich nicht nur ergeben, welche Grundstücke der Gemeinde gehören oder bei welchen das Eigentum der Gemeinde

[47] s. 6. Tätigkeitsbericht unter 12.6.1.3

- etwa wegen noch anhängiger Vermögenszuordnungsverfahren - noch nicht feststeht. Es sollten zudem auch solche Grundstücke mitgeteilt werden, die in der Vergangenheit - z. B. nach dem "Modrow-Gesetz" - an Dritte verkauft worden waren. Dabei sollten auch die Namen der Eigentümer mitgeteilt werden.

In wieder anderen Fällen war strittig, ob die Verwaltung der Gemeindevertretung Haushaltssachbücher der Kämmerei vorlegen durfte oder die Gemeindevertretung den Amtsdirektor verpflichten kann, Gewerbesteuereinnahmen einzelner Gewerbetreibender ohne deren Zustimmung vorzulegen.

Auch wenn bei jeder Anfrage selbstverständlich im Einzelfall zu prüfen ist, welche Informationen die Kommunalverwaltung der Kommunalvertretung zur Verfügung stellen darf und muss, so lassen sich jedoch einige allgemeine Grundsätze aufstellen.

Die Weitergabe von personenbezogenen Informationen durch die Kommunalverwaltung an die jeweilige Vertretungskörperschaft ist nach den für Datenübermittlungen geltenden Vorschriften zu beurteilen. Sowohl Verwaltung als auch die Vertretungskörperschaft sind zwar Organe der gleichen Gemeinde und damit auch derselben öffentlichen Stelle. Daten verarbeitende Stelle im Sinne des § 3 Abs. 4 Nr. 1 BbgDSG ist daher die Gemeinde (Grundsatz der Einheit der Kommunalverwaltung). Auf der anderen Seite ist jedoch nach der Rechtsprechung des BVerfG[48] der Grundsatz der informationellen Gewaltenteilung zu beachten. Danach sind personenbezogene Daten innerhalb der Kommune nach den jeweiligen Aufgaben in den einzelnen Fachämtern zu trennen. Gleiches gilt für das Verhältnis zwischen Gemeindeverwaltung und Gemeindevertretung. Das Datenschutzrecht trägt dem dadurch Rechnung, dass es in § 14 Abs. 5 BbgDSG die Weitergabe personenbezogener Daten innerhalb einer öffentlichen Stelle einer Datenübermittlung zwischen öffentlichen Stellen gleichstellt.

Die Weitergabe von personenbezogenen Informationen an die Gemeindevertretung ist u. a. dann zulässig, wenn eine Rechtsvorschrift dies vorsieht. Die zentrale Rechtsvorschrift dafür ist § 36 Gemeindeordnung (GO). § 36 GO gibt der Gemeindevertretung ein umfassendes Informations- und Auskunftsrecht gegenüber der Gemeindeverwaltung. Dies ist auch notwendig, da die Gemeindevertretung die ihr zustehenden Aufgaben nur dann erfüllen kann, wenn ihr ausreichende Informationen zur Verfügung stehen. Außerdem kann die Gemeindevertretung den Bürgermeister sowie die Gemeindeverwaltung auch nur kontrollieren, wenn sie über das Verwaltungshandeln informiert ist.

---

[48] BVerfG NJW 1988, S. 959

Die Informationsrechte der Gemeindevertretung nach § 36 GO sind jedoch nicht schrankenlos. Vielmehr kann sich die Gemeindevertretung nur solche Informationen von der Gemeindeverwaltung beschaffen, die zur Erfüllung ihrer eigenen Aufgaben erforderlich sind. Dies ergibt sich aus der Vorschrift des § 36 Abs. 3 GO, wonach ein Zusammenhang mit der Vorbereitung oder der Kontrolle von Beschlüssen der Gemeindevertretung bestehen muss. Soweit dabei personenbezogene Daten von Bürgerinnen und Bürgern betroffen sind, folgt dies darüber hinaus aus dem allgemeinen datenschutzrechtlichen Grundsatz, dass die Übermittlung personenbezogener Daten an öffentliche Stellen nur dann zulässig ist, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

Ausgehend davon ist deshalb im Einzelfall immer zu prüfen, ob die von der Gemeindevertretung gewünschten Auskünfte für deren Aufgabenerfüllung wirklich erforderlich sind. Die Aufgaben der Gemeindevertretung ergeben sich vor allem aus dem Katalog in § 35 GO. Sind die Informationen für die Erfüllung dieser Aufgaben erforderlich, ist der Bürgermeister bzw. Amtsdirektor verpflichtet, Auskünfte zu erteilen oder Akteneinsicht zu gewähren.

In vielen Fällen benötigt die Gemeindevertretung gar keine personenbezogenen Daten. Daher ist es aus unserer Sicht völlig unbedenklich, wenn sich die Gemeindevertretung beispielsweise eine Übersicht übergeben lässt, aus der hervorgeht, welche Grundstücksflächen sich im Eigentum der Gemeinde befinden. Dabei dürften personenbezogene Daten von Bürgern in der Regel keine Rolle spielen. Eine solche Übersicht ist erforderlich, damit die Gemeindevertretung sich über den Vermögensbestand der Gemeinde umfassend informieren kann, um den Haushalt verabschieden zu können. Das Gleiche gilt für die Vorlage der Haushaltssachbücher der Kämmerei.

Zulässig ist es z. B. auch, dass sich die Gemeindevertretung eine Aufstellung derjenigen Grundstücke zur Verfügung stellen lässt, die verkauft werden sollen oder bei denen das Eigentum der Gemeinde strittig ist. Dazu gehören z. B. solche, bei denen eine Vermögenszuordnung beantragt ist. Falls dabei auch personenbezogene Daten von Bürgern, insbesondere von aktuellen Eigentümern, potentiellen Käufern o. ä., weitergegeben werden sollen, ist zu beachten, dass sie nur insoweit übermittelt werden dürfen, wie es für die Erfüllung der Aufgaben nach § 35 GO erforderlich ist. Es ist vor allem darauf Wert zu legen, dass die Erforderlichkeit hinsichtlich jedes Grundstückes einzeln geprüft werden muss. Kommt die Gemeindeverwaltung zu dem Ergebnis, dass in solchen Fällen personenbezogene Daten an die Gemeindevertretung zu übermitteln sind, so sollte gemäß § 44 Satz 2 GO jedenfalls die Öffentlichkeit von der Sitzung ausgeschlossen werden. Die betroffenen Bürger haben dann ein berechtigtes Interesse daran, dass die Gemeindevertretung nicht öffentlich berät.

Nicht zulässig ist es, wenn die Gemeindeverwaltung der Gemeindevertretung eine Übersicht zur Verfügung stellt, aus der alle Eigentümer hervorgehen, deren Grundstücke eine bestimmte Größe überschreiten oder die mehrere Grundstücke innehaben. Ebenso gilt dies für die Weitergabe einer Übersicht, aus der alle bisher verkauften Grundstücke der Gemeinde hervorgehen. Dabei spielt es keine Rolle, ob die Verkäufe nach dem "Modrow-Gesetz" stattgefunden haben oder auf anderer Rechtsgrundlage.

Anders ist es, wenn einzelne Verkaufsvorgänge bei Verkäufen gemeindeeigener Grundstücke geprüft werden sollen, bei denen noch Möglichkeiten der Rückabwicklung der Verträge bestehen. Für solche Fälle ist nach unserer Auffassung eine Zuständigkeit der Gemeindevertretung nach § 35 GO gegeben. Bei der Beratung solcher Vorgänge sollte aber auf jeden Fall die Öffentlichkeit gem. § 44 Satz 2 GO ausgeschlossen werden, da hier regelmäßig davon auszugehen ist, dass sensible Daten von Bürgerinnen und Bürgern, vor allem der Vertragspartner, übermittelt werden.

Schließlich gibt es Fälle, in denen personenbezogene Daten zwar zur Aufgabenerfüllung der Gemeindevertretung erforderlich sein können, Rechtsvorschriften einer Weitergabe jedoch entgegenstehen. Dies gilt zum Beispiel für Daten, die unter das Steuergeheimnis nach § 30 Abgabenordnung fallen. Deshalb kann sich die Gemeindevertretung nicht Zahlen über einzelne Gewerbetreibende übergeben lassen, es sei denn die Betroffenen haben darin eingewilligt.

Begehren Gemeindevertreter Akteneinsicht bei der Verwaltung, so ist ihnen Gelegenheit zu geben, in zumutbarer Weise ihre Rechte wahrzunehmen. Dabei ist zu beachten, dass die Gemeindevertreter ehrenamtlich tätig sind und oft einer beruflichen Tätigkeit nachgehen. Dies sollte bei der Terminfestlegung berücksichtigt werden. Aus unserer Sicht besteht darüber hinaus kein qualitativer Unterschied zwischen Akteneinsicht und der Herausgabe von Kopien durch die Verwaltung. Bei der Weitergabe von Kopien mit personenbezogenen Daten sind sie darauf hinzuweisen, dass sie diese vertraulich behandeln müssen.

Insgesamt sollte die Gemeindeordnung bei nächster Gelegenheit um datenschutzrechtliche Regelungen ergänzt werden, wie sie das Datenschutzgesetz für das Verhältnis zwischen Landesregierung und Landtag bereits enthält.

4.6.2 Datenschutz und Akteneinsicht im kommunalen Satzungsgebungsverfahren

Die Gemeinde beabsichtigte, die das Grundstück einer Petentin erschließende Straße zu erneuern. Um die Anwohner der Straße an den Erschließungskosten zu beteiligen, wollte die Gemeinde eine Satzung verabschieden, in der die Erschließungsbeiträge für die Einwohner festgesetzt werden sollten. In der Satzung sollte u. a. festgelegt werden, nach welchem Schlüssel die Erschließungsbeiträge auf die Anwohner verteilt werden. Die Petentin hatte Zweifel, dass es bei der Festlegung des Verteilungsschlüssel gerecht zugehen würde und wollte deshalb Einsicht in die entsprechenden Unterlagen in der Gemeindeverwaltung nehmen. Die Gemeindeverwaltung hat ihr die Akteneinsicht unter Hinweis auf datenschutzrechtliche Bestimmungen verwehrt.

Die Entscheidung der Gemeinde, keine Akteneinsicht zu gewähren, war nur teilweise korrekt. Die Einsichts- und Informationsrechte der Bürgerinnen und Bürger sind in jeder Phase des Satzungsgebungsverfahrens unterschiedlich ausgestaltet. So bestehen vor Erlass der Satzung andere Rechte, als nach diesem Zeitpunkt. Bei der Ausführung der Satzung im Einzelfall bestehen wiederum andere Möglichkeiten, Informationen von der Gemeinde zu erlangen.

Nach dem Kommunalabgabengesetz für das Land Brandenburg können Erschließungsbeiträge nur aufgrund einer gemeindlichen Satzung erhoben werden. Das Verfahren, nach dem eine Gemeinde Satzungen verabschiedet, ist in der Gemeindeordnung (GO) geregelt.

Solange die Satzung noch nicht verabschiedet ist, enthalten die Vorschriften der GO keine besonderen Regelungen zum Akteneinsichtsrecht durch die Bürger. Das Akteneinsichts- und Informationszugangsgesetz gilt für diesen Teil des Verfahrens ebenfalls nicht, da es nur bei abgeschlossenen Verfahren anwendbar ist. Dies bedeutet aber nicht, dass die Bürgerinnen und Bürger in dieser frühen Phase des Verfahrens keine Informationsmöglichkeiten haben. Sie können an den Gemeindevertretersitzungen teilnehmen, in denen Satzungen beraten werden, weil sie grundsätzlich öffentlich sind.

Wenn die Satzung erlassen ist, ist die Gemeinde nach der GO verpflichtet, diese öffentlich bekannt zu machen. Darüber hinaus gibt die Gemeindeordnung jeder Bürgerin und jedem Bürger das Recht, Satzungen einschließlich aller Anlagen und Pläne innerhalb der öffentlichen Sprechzeiten der Verwaltung einzusehen und sich Abschriften davon geben zu lassen. In dem von der Petentin geschilderten Fall wäre es damit insbesondere auch möglich, den Schlüssel für die Aufteilung der Erschließungsbeiträge zu prüfen und nachzuvollziehen. Datenschutzrechtliche

Bestimmungen können dem grundsätzlich nicht entgegen gehalten werden. Satzungen enthalten keine personenbezogenen Daten, da sie wie Gesetze und Rechtsverordnungen abstrakt formuliert und für eine unbestimmte Zahl von Personen gültig sind.

Für die Anwendung im Einzelfall muss die Satzung regelmäßig durch einen Verwaltungsakt umgesetzt werden. So wird beispielsweise der konkret von einem Grundstückseigentümer zu zahlende Erschließungsbeitrag mit einem Beitragsbescheid festgesetzt. In diesem Verfahren steht den betroffenen Bürgerinnen und Bürgern ebenfalls ein Akteneinsichtsrecht zu. Rechtsgrundlage dafür ist § 29 Brandenburgisches Verwaltungsverfahrensgesetz. Nach dieser Vorschrift hat jeder Beteiligte an einem Verwaltungsverfahren einen Anspruch auf Akteneinsicht, soweit die Kenntnis der in den Unterlagen enthaltenen Informationen zur Verteidigung seiner rechtlichen Interessen erforderlich ist. Bestehen im vorliegenden Fall also Zweifel, dass dem Beitragsbescheid ein nicht ordnungsgemäßer Verteilungsschlüssel für die Heranziehung zu den Erschließungsbeiträgen zu Grunde liegt, bezieht sich der Anspruch des Betroffenen auf Akteneinsicht auf jeden Fall auf die Unterlagen, aus denen sich ergibt, welche Kriterien der Berechnung zu Grunde gelegt worden sind. Davon sind auch Unterlagen aus dem Satzungsgebungsverfahren umfasst.

Sind in solchen Unterlagen auch personenbezogene Daten Dritter, z. B. anderer Straßenanlieger, enthalten, ist die Gemeinde nicht verpflichtet, Akteneinsicht zu gewähren. In Fällen wie dem hier geschilderten ist es in aller Regel aber auch gar nicht erforderlich, dass der Auskunftsbegehrende von personenbezogenen Daten Dritter Kenntnis erlangt. Normalerweise wird dem Informationsinteresse der Beteiligten damit Genüge getan sein, dass sie die der Entscheidung zu Grunde liegenden Kriterien nachvollziehen können. Auf solche Informationen besteht - wie dargestellt - ein Anspruch des betroffenen Bürgers.

Der gleiche Anspruch auf Akteneinsicht steht den Bürgerinnen und Bürgern auch im Widerspruchsverfahren zu. Ebenso enthält die Verwaltungsgerichtsordnung für das Klageverfahren einen speziellen umfassenden Akteneinsichtsanspruch.

Bei der Schaffung von kommunalen Satzungen, aber auch bei ihrer Anwendung im Einzelfall bestehen in jeder Phase Akteneinsichts- und Informationsansprüche der Bürgerinnen und Bürger oder der Öffentlichkeit. Datenschutzrechtliche Bestimmungen können dem nicht entgegenstehen, soweit sich keine personenbezogenen Daten Dritter in den Unterlagen befinden.

5 Justiz und Europaangelegenheiten

5.1 Neues zum Täter-Opfer-Ausgleich

Beim sogenannten Täter-Opfer-Ausgleich wird der staatliche Strafverfolgungsanspruch zu Gunsten einer angestrebten Einigung zwischen den Opfern einer Straftat und deren Tätern zurückgestellt. Nicht die Strafe und das Strafverfahren stehen im Vordergrund, sondern die Möglichkeit, beispielsweise durch Wiedergutmachung des Schadens oder einer Versöhnung eine Lösung herbeizuführen, die die Verhängung einer Strafe überflüssig macht. Im Ergebnis ist hierdurch einerseits den Interessen des Opfers besser gedient und andererseits leistet die Täterin oder der Täter Sühne, ohne formal vorbestraft zu sein. Insbesondere im Bereich der Jugenddelinquenz erscheint dieses Verfahren geeignet, die Zwangsläufigkeit krimineller Karrieren zu durchbrechen und langfristig die Täter zu resozialisieren, ohne dabei die Interessen der Opfer unberücksichtigt zu lassen. Das Land Brandenburg nimmt hier eine Spitzenposition ein: 1/3 aller in den Bundesländern zu Stande gekommenen Schlichtungen kamen hier zu Stande[49].

[49] *s. dazu 5. Tätigkeitsbericht, Pkt. 4.2*

Datenschutzrechtlich war in erster Linie die Frage zu klären, wie mit den Daten der Beteiligten und vor allem der Opfer umzugehen ist. Ein Täter-Opfer-Ausgleich kann nur erfolgen, wenn die Opfer mit ihm einverstanden sind, sie mithin darauf verzichten, dass ein strafrechtliches Verfahren gegen die Täter durchgeführt wird. Diesem tragen die neuen Regelungen zum Täter-Opfer Ausgleich in den §§ 153 a ff. der Strafprozessordnung (StPO)[50] dahingehend Rechnung, dass ein Ausgleich gegen den Willen des Verletzten nicht stattfinden soll. Erst wenn das sichergestellt ist, erlauben sie die Übermittlung von personenbezogenen Daten, soweit sie zur Durchführung eines Täter-Opfer-Ausgleichs erforderlich sind, an die damit beauftragten Stellen, die auch freie (nichtstaatliche) Träger sein können.

Zwar sieht das Gesetz vor, dass die Opfer einer Datenweitergabe an Dritte zur Durchführung des Täter-Opfer-Ausgleichs ausdrücklich widersprechen müssen, wenn sie dies verhindern wollen. Die Konferenz der Datenschutzbeauftragten hatte sich in einer Entschließung während des Gesetzgebungsverfahrens demgegenüber für eine Einwilligungslösung zu Gunsten der Opfer eingesetzt[51], die nicht Eingang in das Gesetz gefunden hat. Andererseits ist zu begrüßen, dass die Vorschläge des Bundesrates, der die Datenübermittlung sogar gegen den Willen der Opfer zulassen wollte, ebenfalls unberücksichtigt geblieben sind.

5.2 Alter Hut mit neuen Löchern

Der unzureichende Rückfluss von Informationen über den Ausgang des staatsanwaltschaftlichen Ermittlungsverfahrens an die Polizei war schon in der Vergangenheit immer wieder Thema in unseren Tätigkeitsberichten[52]. Dass das sog. Rückmeldeverfahren über den Verfahrensausgang von der Staatsanwaltschaft an die Polizeibehörden nicht so funktioniert, wie es im Interesse des Persönlichkeitsschutzes der Betroffenen erforderlich wäre, ist ein alter Hut. Bei der diesjährigen Prüfung von Kriminalakten[53] haben wir nun in dem alten Hut neue Löcher entdeckt.

Das 1995 zwischen Polizei- und Justizbehörden festgelegte Verfahren ließ eigentlich erwarten, dass die datenschutzrechtlichen Belange der Betroffenen angemessen gewahrt würden. Danach übergeben die

---

50 Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20.12.1999, BGBl. I S. 2491 f.

51 s. Dokumente zum Datenschutz 1999, Teil A III

52 *s. 2. Tätigkeitsbericht unter Pkt. 3.6.2.2, 3. Tätigkeitsbericht unter Pkt. 4.1.4, 4. Tätigkeitsbericht unter Pkt. 4.3 und 5. Tätigkeitsbericht unter Pkt. 4.2.2*

53 *s. oben Pkt. 4.1.4*

Polizeidienststellen der Staatsanwaltschaft die Ermittlungsvorgänge zusammen mit einem Formular, auf dem der Staatsanwalt nur noch Aktenzeichen und Verfahrensausgang einschließlich Rechtsgrundlage bei Verfahrenseinstellung eintragen muss. Bei der Prüfung von Kriminalakten in einem Polizeipräsidium fanden wir zahlreiche Formulare, auf denen zwar die Einstellung des Ermittlungsverfahrens einschließlich Aktenzeichen vermerkt war, die Rechtsgrundlage für die Verfahrenseinstellung jedoch fehlte. Solche unzulänglich ausgefüllten Mitteilungen der Staatsanwaltschaft haben in datenschutzrechtlicher Hinsicht gravierende Auswirkungen auf die Persönlichkeitsrechte der Betroffenen. Sie beeinträchtigen aber auch die Verlässlichkeit der kriminalpolizeilichen Sammlungen. Statt die im Zusammenhang mit dem Ermittlungsverfahren gespeicherten Daten zu löschen, weil der Tatverdacht sich nicht bestätigt und die Staatsanwaltschaft das Verfahren daher nach § 170 Abs. 2 StPO eingestellt hat, werden diese Daten bei der Polizei weiter gespeichert und genutzt. Dies ist aber nur nach Verfahrenseinstellungen aus anderen Gründen zulässig.

Solche Mitteilungen ohne Angabe des Einstellungsgrundes stehen im Widerspruch zum Justizmitteilungsgesetz (JuMiG). Darin ist zum Umfang der Mitteilung vorgeschrieben, dass die Polizeibehörde nicht nur über die Entscheidung der Staatsanwaltschaft selbst, sondern auch über die Gründe unterrichtet werden muss, falls dies erforderlich ist. Bei Verfahrenseinstellungen durch die Staatsanwaltschaft ist die Angabe der Rechtsgrundlage, auf der die Einstellung beruht, geboten, weil anderenfalls die Polizei nicht in der Lage ist, daraus Rückschlüsse für die Erforderlichkeitsprüfung der im Zusammenhang mit dem Ermittlungsverfahren erhobenen und gespeicherten Daten zu ziehen.

Wir haben die zuständige Staatsanwaltschaft aufgefordert, dafür Sorge zu tragen, dass den Polizeibehörden zukünftig auch die Rechtsgrundlage der Verfahrenseinstellungen mitgeteilt wird. Dem ist sie mit einer Hausverfügung unterdessen nachgekommen.

Für die Aufbewahrung und Nutzung von Informationen aus Ermittlungsverfahren bei den Polizeibehörden, die gem. § 170 Abs. 2 StPO von der Staatsanwaltschaft eingestellt worden sind, gibt es keine Rechtsgrundlage. Sie sind rechtswidrige Eingriffe in die Persönlichkeitsrechte der Betroffenen, zu deren Vermeidung die Staatsanwaltschaften das Ihre beitragen müssen.

5.3 Offenheit auch im geschlossenen Vollzug möglich

Der Strafvollzug ist notwendigerweise mit einer Vielzahl von Reglementierungen und Einschränkungen für die Rechte der Insassen verbunden. Doch gerade auch unter Einbeziehung des Resozialisierungsgedankens ist zu beachten, dass auch die Strafgefangenen nicht rechtlos sind. Immer wieder werden in diesem Zusammenhang Fragen nach dem Inhalt der sogenannten Gefangenen-Personalakten und den Möglichkeiten, in diese Einsicht zu nehmen, gestellt.

Hier finden überwiegend die speziellen Regelungen der §§ 179 bis 187 des Strafvollzugsgesetzes Anwendung, die insoweit Vorrang vor den allgemeinen Vorschriften der Datenschutzgesetze haben. Grundsätzlich dürfen auch danach nur solche Daten aufgenommen werden, die unmittelbar für den Strafvollzug benötigt werden. Es sollte davon Abstand genommen werden, weitere Daten nach Maßgabe einer freiwilligen Einwilligung der betroffenen Strafgefangenen in die Akten aufzunehmen, da in der besonderen Situation der Strafhaft bei den Betroffenen schnell der Eindruck entstehen könnte, dass aus der Verweigerung von Daten Nachteile folgten, obwohl es zu deren Angabe keine Verpflichtung gibt .

Ferner müssen Informationen, die im Zusammenhang mit der Beratung durch in den Vollzugsanstalten tätige Sozialarbeiter und Psychologen anfallen, getrennt von den allgemeinen Gefangenen-Personalakten aufbewahrt werden.

Dergestalt kann auch das für Strafgefangene in diesen Fällen geltende besondere Beratungsgeheimnis am besten gewahrt werden. Dieses darf nur ausnahmsweise unter den Gesichtspunkten der besonderen Verhältnisse des Strafvollzugs durch Mitteilungen an die Anstaltsleitung eingeschränkt werden, soweit es für die Aufgabenerfüllung einer Vollzugsbehörde oder zur Abwehr von erheblichen Gefahren für Leib und Leben des Gefangenen oder Dritter erforderlich ist.

Im Übrigen haben auch Strafgefangene das Recht, zu erfahren, welche personenbezogene Daten über sie gespeichert sind. Soweit eine bloße Auskunft nicht zur Wahrnehmung der rechtlichen Interessen der Strafgefangenen ausreicht, steht ihnen darüber hinaus ein Akteneinsichtsrecht zu.

Im Bereich der Untersuchungshaft spielt darüber hinaus die Unschuldsvermutung zu Gunsten des Untersuchungshäftlings eine besondere Rolle. Die Bundesregierung hat einen Gesetzentwurf zur Regelung des Vollzugs der Untersuchungshaft vorgelegt, der dem durch differenzierende Regelungen zur Verarbeitung von Häftlingsdaten Rechnung trägt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dies in

einer Entschließung begrüßt und sich zugleich gegen Änderungsvorschläge des Bundesrates ausgesprochen, die das staatliche Vollzugsinteresse einseitig in den Vordergrund stellen. Das Gesetzgebungsverfahren ist noch nicht abgeschlossen.

Auch unter den besonderen Verhältnissen des Strafvollzugs dürfen die Rechte der Strafgefangenen nur soweit wie nötig eingeschränkt werden. Für den Bereich des Schutzes der Persönlichkeitsrechte bedeutet dieses für den Regelfall einen Anspruch auf Wahrung von Beratungsgeheimnissen bei der Beratung durch Sozialarbeiter und Psychologen sowie ein Recht auf Auskunft in Bezug auf die eigenen persönlichen Daten in den Gefangenen-Personalakten.

5.4 Persönlichkeitsrechte beim Wäschewaschen

Eine Justizvollzugsanstalt lässt die gesamte in ihrem Bereich anfallende Wäsche - so auch die persönliche Wäsche der Strafgefangenen - in einer externen Wäscherei waschen. Die Strafgefangenen mussten dabei ihren Namen auf dem Auftragsschein angeben. Da es sich bei der Stadt, in der die Vollzugsanstalt liegt, lediglich um eine Gemeinde mittlerer Größenordnung handelt, kann es bei dieser Praxis dazu kommen, dass Menschen, die nicht zum Personal der Vollzugsanstalt gehören, erfahren, wer aus ihrer örtlichen Umgebung eine Haftstrafe verbüßen muss. Dies trifft insbesondere auch die am Ort lebenden Familienangehörigen der Strafgefangenen.

Rechtlich ist die Bekanntgabe des Namens in Verbindung mit der Inhaftierung als eine Beeinträchtigung des Persönlichkeitsrechts und insbesondere des Grundrechts auf informationelle Selbstbestimmung zu qualifizieren. Beides sind Rechte, die auch Inhaftierten zustehen. Ein Eingriff bedürfte einer rechtlichen Grundlage und müsste selbst dann den Grundsätzen der Verhältnismäßigkeit entsprechen, d.h. die handelnde staatliche Stelle muss stets bemüht sein, so wenig wie möglich in die Rechte der Betroffenen einzugreifen und bei Vorhandensein andere zur Zielerreichung geeignete, aber weniger einschneidende Maßnahmen zu ergreifen.

Die Leitung der Vollzugsanstalt begründete die Notwendigkeit der Namensangabe zunächst damit, dass die Gefangenen selbst die Auftraggeber seien und nicht etwa die Vollzugsanstalt, es mithin notwendig sei, deutlich zu machen, wer der konkrete Vertragspartner der Wäscherei werde. Erst im Nachgang erklärte sich die Haftanstalt bereit, eine andere Form der Auftragsabwicklung anzubieten, die den Interessen der Strafgefangenen besser gerecht wird, weil die namentliche Auftragsvergabe an die Wäscherei vermieden wird. In der Justizvollzugsanstalt wird

nunmehr ein Auftragsbuch geführt, in dem die Aufträge mit fortlaufender Nummer notiert und anschließend auf dem Auftragsschein für die Wäscherei vermerkt werden.

Dieses erfreuliche Beispiel zeigt, wie es bei einmal gewecktem Problembewusstsein und vorhandener Bereitschaft, geeignete Lösungswege zu finden, mit nur geringstem Mehraufwand möglich ist, die Rechte von Betroffenen und ihrer Angehörigen besser zu wahren.

5.5 Guter Rat tut Not

Dass an den Berufsstand der Anwälte in Hinsicht ihrer Unbescholtenheit und persönlichen Integrität besondere Anforderungen zu stellen sind, ist einleuchtend, schließlich sind sie auch Organe der Rechtspflege in der Bundesrepublik Deutschland.

Daher wird mittels eines Fragebogens bei der Zulassung zur Rechtsanwaltschaft des Landes Brandenburg auch nach den möglichen Verstrickungen der Antragsteller in die Tätigkeit des Ministeriums für Staatssicherheit bzw. des Amtes für Nationale Sicherheit der ehemaligen DDR gefragt, um die sogenannte Gauck-Abfrage zu ermöglichen. Gedeckt wird dieses Vorgehen durch die Bundesrechtsanwaltsordnung (§ 7), nach der die Zulassung zur Rechtsanwaltschaft zu versagen ist, wenn sich Antragssteller eines Verhaltens schuldig gemacht haben, das sie zur Ausübung des Rechtsanwaltsberufs unwürdig erscheinen lassen, wozu im Einzelfall auch eine Tätigkeit für eine der beiden genannten Stellen führen kann.

Dass dem Fragebogen die Rechtsgrundlage nicht zu entnehmen war, ist nicht mit den Grundsätzen des Brandenburgischen Datenschutzgesetztes zu vereinbaren. Danach (§ 12 Abs. 3 BbgDSG) soll jemand, von dem die Preisgabe persönlicher Daten gefordert wird, über den Verwendungszweck und die möglichen Empfänger der Daten ausdrücklich aufgeklärt werden. Es sind die rechtlichen Grundlagen darzulegen und soweit die Angabe der Daten freiwillig erfolgen sollte, ist auf die Freiwilligkeit und die Folgen einer möglichen Nichtangabe hinzuweisen. Damit die Betroffenen ihre Verpflichtungen und die Folgen ihres Verhaltens absehen können, muss diese Aufklärung vor Abgabe ihrer Daten, d. h. spätestens zusammen mit der Anforderung der Daten - hier der Zusendung des Fragebogens - geschehen.

Das leuchtete auch der für das Rechtsanwaltszulassungsverfahren zuständigen Stelle beim Oberlandesgericht Brandenburg ein, die aufgrund unseres Hinweises nunmehr zusammen mit der Zusendung des Fragebogens eine den Erfordernissen des Brandenburgischen Datenschutzgesetzes entsprechende Aufklärung vornimmt.

Auch wenn es eine gesetzliche Pflicht für die Preisgabe persönlicher Daten gibt, müssen die Betroffenen zuvor über die gesetzlichen Grundlagen und Verwendungszwecke aufgeklärt werden. Das folgt aus dem rechtsstaatlichen Gebot der Transparenz staatlichen Handelns, was u. a. durch § 12 Abs. 3 Brandenburgisches Datenschutzgesetz konkretisiert wird. Nur so kann eine betroffene Person entscheiden, ob sie der Forderung folgen oder gegen sie gegebenenfalls mit rechtlichen Mitteln vorgehen will.

5.6 Weniger ist mehr

Der Präsident des Brandenburgischen Oberlandesgerichts wandte sich mit der Frage an uns, ob die Verwendung der im Gerichtsbezirk üblichen Empfangsbestätigungen, mit deren Rücksendung u. a. Rechtsanwaltspraxen den Erhalt von gerichtlichen Schriftstücken bescheinigen, datenschutzgerecht sei.

Die Empfangsbestätigungen sind als Postkarten gestaltet und enthalten je nach Ausfertigung unterschiedliche personenbezogene Daten, die das gerichtliche Verfahren berühren. Enthalten sind beispielsweise Angaben über die Verfahrensbeteiligten, die Bezeichnung des Entscheidungsgegenstands, das Geschäftszeichen des Gerichts, oder Hinweise, ob es sich bei dem Verfahren um eine Straf- oder Freiheitsentziehungssache handelt.

Zwar kann geltend gemacht werden, dass die Wahrnehmung dieser Informationen lediglich durch Bedienstete der Post sowie der Post- und Geschäftsstellen der Gerichte möglich ist und dass dieser Personenkreis zudem einer strafrechtlich bewehrten Verschwiegenheitspflicht unterliegt, doch ändert das nichts an dem Umstand, dass die Kenntnisnahme dieser Informationen nicht für die Erfüllung der jeweiligen Aufgabe, dem ordnungsgemäßen Zustellen der Post, erforderlich ist. Getreu dem Grundsatz, dass nur die für die Aufgabenerfüllung zwingend erforderlichen personenbezogenen Daten verarbeitet werden dürfen, bieten sich zwei Wege einer datenschutzgerechteren Gestaltung des Verfahrens an:

Erstens die Reduzierung der verwendeten Daten: Es könnte lediglich das Geschäftszeichen verwendet werden, sodass nach außen nur noch bestätigt werden würde, ein Schriftstück eines Gerichts zu einem Aktenzeichen erhalten zu haben. Zumindest Gerichtsbedienstete könnten allerdings bei dieser Handhabung anhand des Geschäftszeichens noch weitere Informationen über die Art des Verfahrens u. Ä. erschließen.

Zweitens der Verzicht auf die Verwendung offener Postkarten: Der Empfänger könnte aufgefordert werden, die Empfangsbestätigungen in einem verschlossenen Umschlag zu versenden, was den Vorzug hätte, dass der Umfang der Informationen nicht verändert werden müsste und dass wirklich erst der Empfänger den konkreten Inhalt der Nachricht wahrnimmt.
Insgesamt verdient der zweite Lösungsweg daher den Vorzug.

Der Präsident des Oberlandesgerichts ist unserem Vorschlag dahingehend gefolgt, dass er einen Modellversuch gestartet hat, in dem die Empfänger von gerichtlichen Schriftstücken zumindest in Straf- und Freiheitsentziehungssachen gebeten werden, die Bestätigung des Erhalts in einem geschlossenen Umschlag zurückzusenden.

Gerade in solch empfindlichen Bereichen wie der Strafjustiz ist es ratsam, möglichst restriktiv mit der Verwendung von Daten umzugehen und dafür Sorge zu tragen, dass auch die bei der Zustellung von Schriftstücken beteiligten Personen möglichst wenig Gelegenheit zum Erhalt der Kenntnis von Daten bekommen, die sie für ihre Aufgabenerfüllung nicht benötigen. In diesem Sinne bedeutet hier ein Weniger an Daten ein Mehr an Persönlichkeitsschutz.

5.7 Auswertung strafrechtlicher Rehabilitierungsakten für wissenschaftliche Zwecke

Ein Doktorand hatte im Rahmen seines Promotionsvorhabens Einsicht in die beim Landgericht archivierten strafrechtlichen Rehabilitierungsakten beantragt und sich als Rechtsgrundlage auf die Richtlinien für Straf- und Bußgeldverfahren berufen. Das Landgericht bat uns um Stellungnahme zum datenschutzrechtlichen Aspekt des Einsichtsantrages.

Am 8. April 1999 hat das Ministerium der Justiz und für Bundes- und Europaangelegenheiten eine Allgemeine Verfügung über die geschäftliche Behandlung von Anfragen und Auskunftsersuchen zu wissenschaftlichen Zwecken erarbeitet, zu der wir im Entwurfsstadium Stellung genommen haben[54]. Durch die Verfügung wird die Entscheidung zu Anfragen, Auskunftsersuchen und Anträgen auf Akteneinsicht, die sich bislang das Ministerium vorbehalten hat,

[54] Justizministerialblatt, 1999 S. 59

grundsätzlich den Behördenleitern übertragen. Den Erfordernissen des Brandenburgischen Datenschutzgesetzes (BbgDSG), insbesondere § 28 BbgDSG, wird Rechnung getragen.

Da es sich bei dieser Richtlinie um eine untergesetzliche Vorschrift handelt, ist zunächst § 28 BbgDSG vorrangig heranzuziehen, während die hier ebenfalls einschlägige Richtlinie für das Straf- und Bußgeldverfahren (Nr. 185 a) ergänzend Berücksichtigung findet. Nach § 28 Abs. 1 BbgDSG dürfen öffentliche Stellen personenbezogene Daten zu wissenschaftlichen Zwecken verarbeiten, wenn die Betroffenen eingewilligt haben. Soweit mit einer solchen Einwilligungserklärung nicht in dem für das Forschungsvorhaben nötigen Umfang zu rechnen ist, müssen die Voraussetzungen des § 28 Abs. 2 BbgDSG vorliegen. Danach dürfen öffentliche Stellen ausnahmsweise personenbezogene Daten ohne Einwilligung für ein bestimmtes Forschungsvorhaben an andere Stellen oder Personen zum Forschungszweck übermitteln, wenn die zuständige oberste Aufsichtsbehörde festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Dissertationen können im Einzelfall als ein Forschungsvorhaben i. S. d. § 28 Abs. 2 BbgDSG aufgefasst werden.

Das Landgericht hat unsere datenschutzrechtlichen Hinweise an den Doktoranden weitergeleitet:

- Die erlangten personenbezogenen Informationen sind von dem Assessor so bald wie möglich zu anonymisieren und dürfen nur zu dem Zweck dieses Forschungsvorhabens verwendet werden. Auswertungsergebnisse dürfen nur in anonymisierter Form weitergegeben und veröffentlicht werden.

- Die Einsichtnahme ist auf rechtskräftig abgeschlossene Verfahren zu beschränken. Darüber hinaus sollte in jedem Einzelfall geprüft werden, ob entgegenstehende Interessen ersichtlich sind.

- Die Einsichtnahme in die strafrechtlichen Rehabilitierungsakten sollte möglichst nur in nicht öffentlich zugänglichen Räumen der Akten führenden Dienststelle erfolgen.
- Die Abgabe einer Verschwiegenheitserklärung durch den Wissenschaftler ist erforderlich.

Eine Auswertung von strafrechtlichen Rehabilitierungsakten für eine wissenschaftliche Untersuchung, an der ein überwiegendes öffentliches Interesse besteht, ist unter engen Voraussetzungen auch ohne Einwilligung der Betroffenen zulässig.

6 Bildung, Jugend und Sport

6.1 Kontrollbesuche in Oberstufenzentren

Nachdem wir uns bereits 1998 Jahr über die Organisation und Arbeitsweise eines Oberstufenzentrums informiert hatten[55], überprüften wir im Berichtszeitraum weitere Oberstufenzentren. Dabei zeigten sich ähnliche Mängel.

Zum Teil gibt es an Oberstufenzentren keinen internen Schuldatenschutzbeauftragten, der gem. § 11 Abs. 1 Datenschutzverordnung Schulwesen (DSV) für die Einhaltung des Datenschutzes in den Schulen verantwortlich ist. Der Vorschlag eines Schulleiters, sich selbst mit dieser Aufgabe zu betrauen, steht im Widerspruch zu § 11 Abs. 1 DSV. Denn danach muss der Schulleiter ein anderes Mitglied der Schulleitung mit dieser Aufgabe betrauen, um einen Interessenkonflikt zwischen Schulleitungsaufgaben und Lösung datenschutzrechtlicher Probleme zu vermeiden. Der interne Datenschutzbeauftragte muss seine Funktion unabhängig von der Leitung der jeweiligen öffentlichen Stelle ausüben.

Darüber hinaus gab es teilweise keine Dienstanweisungen zum Datenschutz in der Schule. In anderen Fällen lagen zwar allgemeine Festlegungen vor, die jedoch nicht den Vorgaben der DSV sowie der Verwaltungsvorschriften über Akten an Schulen im Land Brandenburg (VV-Schulakten) genügten.

In mehreren Klassenbüchern wurden Entschuldigungsschreiben gefunden. Diese dürfen dort nicht lose aufbewahrt werden, sondern nur in einer gesonderten Mappe. Gleiches gilt für Atteste und Arbeitsunfähigkeitsbescheinigungen. Soweit es sich um Angaben über gesundheitliche Beeinträchtigungen handelt, sind diese in einem verschlossenen Umschlag in der Schülerakte abzuheften. Nach wie vor enthielten die Klassen- bzw. Notenbücher mehr Daten als in der Anlage 1 Nr. 2 ff. der DSV aufgeführt sind. In mehreren Klassenbüchern war die Anschrift des Ausbildungsbetriebes eingetragen. Die Aufnahme dieser Daten kann nur mit der Einverständniserklärung des jeweiligen Schülers erfolgen, die gleichfalls in die Schülerakte aufzunehmen ist.

Im Übrigen sollen in Klassen- oder Notenbüchern nur solche Daten erfasst werden, die unbedingt zur Aufgabenerfüllung erforderlich sind.

---

[55] *s. Tätigkeitsbericht 1998, Pkt. 8.1*

6.1.1 Akten von Schülerinnen, Schülern und Lehrkräften

6.1.1.1 Informationen an Ausbildungsbetriebe

Will die Berufsschule Daten über Auszubildende an den Ausbildungsbetrieb weitergeben, so benötigt sie dazu die Einwilligung der Auszubildenden. Diese sind zwar selbst im Rahmen des Ausbildungsvertrags und nach dem Berufsbildungsgesetz dazu verpflichtet, den Ausbildungsbetrieb über ihre schulischen Leistungen zu informieren. Um den Berufsschulen aber die Möglichkeit zu geben, bei Bedarf ihrerseits den Ausbildungsbetrieb auch über Fehlzeiten oder Ordnungsmaßnahmen zu informieren, hatte das Ministerium für Bildung, Jugend und Sport 1998 im Rundschreiben 54/98 dies zugelassen, soweit eine gesonderte Einwilligungserklärung des Betroffenen vorliegt[56].

Dies wiederum stieß auf Kritik sowohl bei den Handwerks- als auch den Industrie- und Handelskammern, nach deren Auffassung die Auszubildenden sich nicht durch schlichte Verweigerung oder Widerruf der Einwilligung ihren Pflichten aus dem Ausbildungsverhältnis entziehen können. Nunmehr wird überwiegend schon in die Ausbildungsverträge ein Passus aufgenommen, in dem sich die Auszubildenden mit der Weitergabe ihrer Daten durch das Oberstufenzentrum für den Fall einverstanden erklären, dass sie ihrer eigenen Mitteilungspflicht nicht nachkommen. Dagegen ist aus Sicht des Datenschutzes nichts einzuwenden. Das Ministerium beabsichtigt daher, sein Rundschreiben entsprechend zu ändern.

Auch in diesem Berichtsjahr war die Aufbewahrungsdauer der Kopie der ersten Seite des Ausbildungsvertrages in der Schülerakte ein Problem. Wir hatten zunächst empfohlen, dieses Duplikat nicht länger als ein halbes Jahr in der Schülerakte aufzubewahren. Nach Auffassung der Oberstufenzentren ist dieser Zeitraum zu kurz. Deshalb sollte es mindestens ein Jahr aufbewahrt werden, da dessen Vorlage für die Feststellung der erfolgreichen Absolvierung der Probezeit erforderlich ist und zudem häufig noch ein Jahr nach Beginn der Ausbildung Fachrichtungswechsel erfolgen, deren Abwicklung einen Rückgriff auf die Daten des Ausbildungsvertrages nötig machen. Die Forderung einer längeren Speicherdauer erscheint anhand der praktischen Erfahrungen gerechtfertigt. Deshalb stimmen wir der längeren Aufbewahrungszeit zu.

6.1.1.2 Stammblatt für Lehrkräfte

Ein Schulleiter fragte uns, wer das Stammblatt für Lehrkräfte anzulegen und zu führen habe. Gem. § 9 Abs. 5 DSV dürfen die Schulleitung sowie auf deren Weisung das Schulsekretariat Eintragungen in die Unterlagen der Lehrkräfte

---

[56] s. Tätigkeitsbericht 1998, Pkt. 8.1

(darunter das Stammblatt) und des sonstigen pädagogischen Personals vornehmen. In diese dürfen die Schulleitung, die Leitung des staatlichen Schulamtes sowie die für die Schule zuständige Schulrätin oder der für die Schule zuständige Schulrat Einsicht nehmen. Sie sind bis zum Ausscheiden der betreffenden Person aus der Schule aufzubewahren. Aufbewahrungsort für diese Unterlagen ist stets die Schule, an der die Lehrkräfte zuletzt tätig waren. Nach dem Ausscheiden aus dem Schuldienst sind diese Akten unmittelbar an das staatliche Schulamt abzugeben und dort zu den Personalakten zu nehmen.

6.1.1.3 Alte Aufnahmeanträge

In mehreren Fällen haben wir alte Aufnahmeanträge (z. B. aus dem Jahre 1993) gefunden, die nicht mehr abgeholt worden waren. Diese Unterlagen können vernichtet werden, da nicht mehr damit zu rechnen ist, dass ein Schüler Interesse an der Abholung dieser Schreiben hat. Bei Aufnahmeanträgen abgelehnter Schülerinnen und Schüler aus dem Jahr 1998/99 sind die Betroffenen vor deren Vernichtung in angemessener Frist auf die Möglichkeit der Abholung schriftlich hinzuweisen.

Um den Verwaltungsaufwand zu minimieren, sollte in Zukunft ein Hinweis auf diese Möglichkeit gleich bei der Entgegennahme der Bewerbung etwa im Zusammenhang mit einem Eingangsbestätigungsschreiben oder durch Aushändigung eines Merkblattes erfolgen.

6.1.2 Technisch-organisatorische Aspekte

6.1.2.1 Verwaltungssoftware

Bei den kontrollierten Oberstufenzentren fiel auf, dass noch keine einheitliche Schulverwaltungssoftware zum Einsatz kommt. Meist wurden eigene Tabellen oder Datenbanken aus Standardsoftwareprogrammen zur Vereinfachung des Verwaltungsaufwandes erstellt.

Es war den Schulleitungen zwar bekannt, dass das Ministerium für Bildung, Jugend und Sport eine Landeslizenz des Softwareproduktes "ISL-Schule" besitzt und kostenlos an die Schulen abgibt, jedoch konnte man sich aus verschiedenen Gründen nicht zum Umstieg auf diese Software entschließen. Die Oberstufenzentren monierten, dass es keine Schulungsangebote gebe oder dass die Software noch nicht an die Brandenburgischen Vorschriften angepasst sei. Wir haben uns daraufhin an das Ministerium für Bildung, Jugend und Sport gewandt, um diese Fragen zu klären. Die Antwort steht noch aus. Aus Sicht des Datenschutzes ist der Einsatz der lizenzierten Schulverwaltungssoftware sinnvoll, da so die landesweite Verwendung eines einheitlichen Datensatzes sichergestellt ist und nicht die zusätzliche Speicherung weiterer Daten aufgrund lokaler Gepflogenheiten erfolgen kann.

6.1.2.2 Schulverwaltungsnetz

Die Schulverwaltungen arbeiten zum Teil mit lokalen Netzen. In einem Fall war das lokale Netz mit dem Netz der zum Unterricht benutzten PC's verbunden, was nach § 4 Abs. 1 DSV unzulässig ist, um unbefugte Zugriffe auf die Verwaltungsdaten zu unterbinden. Die umgehende Abhilfe wurde zugesagt.

6.1.2.3 Aktenvernichtung

Mancherorts werden Altakten und sonstige Papiere über Entsorgungsfirmen vernichtet. Die Schulleitung sollte sich vergewissern, dass der Schulträger mit diesen Firmen einen Vertrag abgeschlossen hat, da es sich dabei um eine Datenverarbeitung im Auftrag nach § 11 BbgDSG handelt und Mindeststandards der Datensicherheit und des Datenschutzes einzuhalten sind, die der ausdrücklichen schriftlichen Festlegung bedürfen.

6.1.2.4 Verfahrens- und Anlagenverzeichnis

Nach § 8 BbgDSG hat jede Daten verarbeitende Stelle ein Verfahrens- und Anlagenverzeichnis zu erstellen. An den meisten Schulen lagen diese Verzeichnisse in der alten Fassung (Dateibeschreibung und Geräteverzeichnis) vor. Wir wiesen darauf hin, dass das Ministerium des Innern eine neue Rechtsverordnung zur Ausgestaltung der Verzeichnisse erlassen wird. Diese Verordnung zum Verfahrens- und Anlagenverzeichnis ist inzwischen in Kraft getreten[57].

Es ist grundsätzlich die Aufgabe der Behördenleitung, Datenschutzbestimmungen umzusetzen. Es muss sichergestellt sein, dass die internen Datenschutzbeauftragten ihre Aufgabe frei von Weisungen wahrnehmen und sich ggf. unmittelbar an die Dienststellenleitung wenden können. Daher trägt die Erarbeitung von Dienstanweisungen zum Datenschutz zu einer besseren Umsetzung der Datenschutzbestimmungen bei.

6.2 Schüler sieht seinen eigenen Lebenslauf im Fernsehen

Das Fernsehen filmte ein neu eingerichtetes Computerkabinett einer Gesamtschule. In darauffolgenden Sendungen wurde der Lebenslauf eines nicht anwesenden Schülers gesendet.

[57] VO vom 23.11.1999, GVBl. II S. 646 ff.

Die Einblendung des Schülerlebenslaufes während der Fernsehausstrahlung stellt einen Verstoß gegen § 65 Abs. 6 Brandenburgisches Schulgesetz dar. Nach dieser Vorschrift ist eine Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen nur mit Einwilligung des Betroffenen zulässig. Der Schulleiter hat angekündigt, dafür Sorge zu tragen, dass sich solche Vorfälle in Zukunft an seiner Schule nicht wiederholen werden.

In regelmäßigen Abständen sollte eine Belehrung über die datenschutzrechtlichen Anforderungen nach der Datenschutzverordnung Schulwesen vorgenommen werden. Jede Lehrkraft muss gewährleisten, dass Schülerinnen und Schüler bei der Arbeit am Computer nur Zugriff auf ihre eigenen Daten haben, die bis zum Abschluss der Übungsaufgabe sicher vor dem Zugriff Unbefugter gespeichert und nach deren Abschluss gelöscht werden.

6.3 Heimliche Videoaufzeichnungen von Lehrern

Ein Referent eines Jugendhilfezentrums führte in einer Schule eine interne Fortbildung zum Thema "Video-Interaktions-Begleitung" mit dem Lehrerkollegium durch. Er zeichnete während dieser Veranstaltung die Anwesenden, die mit dem Rücken zur Kamera saßen, ohne deren Kenntnis mit der Kamera auf. Die Aufnahme diente zur Auswertung in einer Supervisionsgruppe des Referenten. Zwei anwesende Lehrkräfte beschwerten sich bei uns über dieses Vorgehen.

Weder das Brandenburgische Schulgesetz noch das Brandenburgische Datenschutzgesetz (BbgDSG) enthalten eine Rechtsgrundlage für die Zulässigkeit von heimlichen Videoaufzeichnungen während einer Fortbildungsveranstaltung. Gem. § 4 Abs. 1 BbgDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene ohne jeden Zweifel eingewilligt hat. Da der Referent zu keinem Zeitpunkt der Veranstaltung auf den Umstand der Videoaufzeichnung der Teilnehmer hingewiesen hat, lag keine Einwilligungserklärung dieses Personenkreises vor.

Da die Betroffenen nicht verpflichtet sind, sich filmen zu lassen, sind Freiwilligkeit und schriftliche Einwilligung Voraussetzung für das Handeln des Referenten. Beim Einholen der Einwilligung ist auch auf den Verwendungszweck der Daten, die Freiwilligkeit der Teilnahme sowie auf etwaige Folgen einer Verweigerung der Einwilligung hinzuweisen. Da dies nicht erfolgt ist, sind die Aufnahmen als ein massiver Eingriff in die Persönlichkeitsrechte zu werten.

Der Leiter des Jugendhilfezentrums teilte uns mit, dass bei gleichgelagerten Vorhaben nunmehr generell das Einverständnis der Beteiligten schriftlich eingeholt wird.

Mit der jeweiligen Schulleitung sollten vor der Videoaufzeichnung von Veranstaltungen die datenschutzrechtlichen Voraussetzungen besprochen werden. Es hat eine Aufklärung i. S. d. § 4 BbgDSG zu erfolgen.

6.4 Datenschutz im Kinder- und Jugendheim

Träger eines von uns kontrollierten Heimes ist das Jugendamt eines Landkreises. Der Landrat hat die Trägeraufgaben auf das Jugendamt delegiert. Die Geschäfte der laufenden Verwaltung werden vom Leiter der Verwaltung der Trägerkörperschaft (Landrat) oder in seinem Auftrag vom Leiter der Verwaltung des Jugendamtes wahrgenommen.

Zur Prüfung der Einhaltung des Datenschutzrechts bei der Erfüllung der übertragenen Aufgaben haben wir die Satzung des Jugendamtes angefordert. Zur Klarstellung der konkreten Zuständigkeitsverteilung zwischen dem Träger und der Heimleitung baten wir ferner um Vorlage des Arbeitsvertrages der Heimleiterin bzw. ihrer Aufgabenbeschreibung.

Das Heim hat uns eine Dienstanweisung des Hauptamtes des Landkreises vorgelegt, die nur allgemein im Rahmen der gesetzlichen Grundlagen auf die datenschutzrechtlichen Vorschriften des Sozialgesetzbuches (SGB) hinweist. Da dies nicht ausreicht, haben wir empfohlen, dass zumindest das Jugendamt eine spezifische Dienstanweisung erstellt, die den gesetzlichen Anforderungen entspricht.

Bei der Prüfung konnte zudem auch nicht abschließend geklärt werden, ob die Betroffenen (Personensorgeberechtigten) bei der Datenerhebung i. d. R. im Jugendamt umfassend aufgeklärt werden. So sind diese z. B. auf die Rechtsgrundlage der Erhebung und auf den Zweck der Verarbeitung oder Nutzung der Daten hinzuweisen. Antragstellerinnen und Antragsteller müssen darüber hinaus erkennen können, wann sie zur Preisgabe ihrer Daten verpflichtet sind und ob diese ihnen freisteht.

Nach Auskunft der Heimleiterin werden im Rahmen der freiwilligen Heimerziehung die Einwilligungserklärungen der Personensorgeberechtigten im Einzelfall eingeholt. Pauschale Einwilligungserklärungen gebe es nicht. Die Eltern hätten Kenntnis darüber, wer am Verfahren beteiligt ist. In einer Akte haben wir dagegen ein Formular mit dem Titel "Antrag und Ermächtigung" entdeckt, in dem die Personensorgeberechtigten einen Antrag auf Gewährung von Hilfen für Erziehung stellen. In diesem Formular heißt es pauschal, dass der Antragsteller Ärzte, Psychologen, Psychotherapeuten und das Gesundheitsamt gegenüber dem Jugendamt von der Schweigepflicht entbindet.

Das ist in dieser Form unzulässig. Erforderliche Einwilligungen sind nicht durch sog. "Pauschaleinwilligungen" zu ersetzen. Einwilligungen sind nur wirksam, wenn sie sich auf den Einzelfall beziehen. Die Betroffenen müssen überschauen können und wissen, welche Daten von ihrer Erklärung betroffen sind. Daher darf das Formular "Antrag und Ermächtigung" nicht weiter verwandt werden.

Sozialdaten, die einem besonderen Vertrauensschutz unterliegen, dürfen in der Betreuungsakte (Handakte des Erziehers) nur so aufbewahrt werden, dass sie dritten Personen nicht ohne Weiteres zugänglich sind. Befugnisse von Vorgesetzten zur Akteneinsicht im Rahmen ihrer Funktion erstrecken sich nicht auf "anvertraute" Daten, die im Zusammenhang mit dem besonderen Betreuungsverhältnis anfallen. Eine Einsichtnahme ist ohne Einwilligungserklärung rechtswidrig und erfüllt u. U. auch Straftatbestände.

In dem Heim wird ein Meldebuch geführt, in das Name, Geburtsname und Vorname des Heimkindes, Geburtsort und -tag, die Adresse der Eltern, woher und durch wen die Entlassung erfolgte, der Tag der Einweisung, wohin die Entlassung erfolgte, der Tag der Entlassung sowie durch wen sie verfügt wurde, eingetragen wird.

Nach dem Brandenburgischen Meldegesetz hat der Heimleiter, wie im Falle einer dauernden Aufnahme in ein Heim, die betreffenden Personen unverzüglich in ein Verzeichnis aufzunehmen. Das Meldebuch wird über mehrere Jahre für jedes Kind fortlaufend geführt. Das Meldegesetz schreibt für diese Daten eine Aufbewahrungsfrist von einem Jahr vor. Danach ist zu prüfen, ob die Daten für die weitere Aufgabenerfüllung noch erforderlich sind. Anderenfalls sind sie unverzüglich zu löschen.

Niemand darf pauschal und losgelöst vom Einzelfall dazu aufgefordert werden, Ärzte, Psychotherapeuten und andere Träger von Berufsgeheimnissen von ihrer Schweigepflicht zu entbinden. Daten, die nicht mehr für die Aufgabenerfüllung gebraucht werden und nicht archivwürdig sind, müssen umgehend vernichtet werden.

6.5 Aufbewahrungsdauer von Jugendamtsakten

Ein Institut, das im Auftrag des Ministeriums für Bildung, Jugend und Sport eine landesweite Empfehlung zur Aktenaufbewahrung in Jugendämtern erarbeiten sollte, wandte sich mit der Bitte an uns, mitzuteilen, welche gesetzlichen Aufbewahrungsvorschriften dabei zu berücksichtigen seien.

Der Betroffene hat Anspruch darauf, dass nach Beendigung der Hilfe seine Sozialdaten gesperrt und die Leistung- und Verwaltungsakten im Regelfall vernichtet werden. Das kann mit Ablauf der Verjährungsfrist für Sozialleistungen erfolgen, die regelmäßig vier Jahre nach Entstehen des Anspruchs endet. In jedem Fall sollten die Akten spätestens nach Ablauf der fünfjährigen Verjährungsfrist für die Verfolgung von Sozialleistungsbetrug vernichtet werden. Unbeschadet dessen sind einzelne Unterlagen u. U. wegen haushaltsrechtlicher Vorschriften auch zehn Jahre aufzubewahren.

Im Falle der Archivierung der Daten unterliegen sie weiterhin dem Sozialgeheimnis gem. § 35 Abs. 1 SGB I. Da gem. § 10 Abs. 4 Brandenburgisches Archivgesetz (BbgArchivG) für die Benutzung von Archivgut, das dem Sozialgeheimnis unterliegende Daten enthält, die Schutzfristen des § 5 Bundesarchivgesetz (BArchG) gelten, darf dieses Archivgut erst 80 Jahre nach Entstehen benutzt werden. Das Landesrecht hat somit für die Nutzung von Archivgut mit Sozialdaten entsprechend § 5 Abs. 2 und 3 BArchG eine 80-jährige Schutzfrist von der Entstehung der Unterlagen an, und eine 30-jährige Schutzfrist vom Tod der Betroffenen an, vorgesehen.

Es gibt keine spezialgesetzlichen Regelungen, wonach in der Jugendhilfe Aufzeichnungen über die Betreuung oder Beratung zu erstellen, aufzubewahren oder zu übermitteln sind. Analog der Rechtsprechung zum Arzt- und Krankenhausrecht ergibt sich jedoch eine Dokumentationspflicht über alle wesentlichen Teilschritte der Betreuung und Beratung (Aufzeichnungen über die Tätigkeit). Diese Pflicht ist eine Nebenpflicht aus dem Auftragsverhältnis mit rechtlichen Konsequenzen für die Einrichtung oder den Dienst hinsichtlich der Beweislast, die Aufgabe sachgerecht und hinreichend erfüllt zu haben. Aufgrund möglicher Schadensersatzansprüche, die noch drei Jahre nach Abschluss einer Betreuung oder Beratung geltend gemacht werden können, ist es zulässig, diese Aufzeichnungen solange gesichert aufzubewahren. Danach sind sie jedoch zu vernichten.

Die u. a. nach § 203 Abs. 1 Nr. 4 StGB geschützten Unterlagen einer Beratungsstelle sind nur in anonymisierter Form gem. § 4 Abs. 2 Nr. 3 BbgArchivG dem zuständigen Archiv anzubieten und zu übergeben. Die Jugendämter sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden, dem zuständigen öffentlichen Archiv entweder unverändert oder anonymisiert anzubieten und - soweit sie archivwürdig sind - zu übergeben.

6.6 Forschungsvorhaben U. MOVE - Jugend und Mobilität

"U. MOVE" heißt eine vom Bundesforschungsministerium geförderte Umfrage zum Mobilitätsverhalten der 15- bis 22-Jährigen. Das mit dem Forschungsprojekt beauftragte private Unternehmen hat uns ein

ausführliches Datenschutzkonzept vorgelegt und um Unterstützung bei der Umsetzung der Befragung von 800 Schülerinnen und Schülern an Brandenburger Schulen gebeten.

Die Umfrage erfolgt in zwei Stufen. Zuerst sollen die Probanden Fragen zu Entscheidungs- und Handlungsmodellen der Verkehrsmittelwahl, zum Lebensstil, zum subjektiven Mobilitätsverhalten sowie zur Bewertung der Verkehrsangebote beantworten. Danach sind mehrere vertiefende Interviews vorgesehen, um weitere Aspekte des Mobilitätsverhaltens zu klären, die sich aus der Auswertung der Fragebögen ergeben haben. Dazu wird auf dem Fragebogen die Adresse erhoben.

Grundsätzlich kann auch an Schulen eine Befragung Minderjähriger zu nichtschulischen Zwecken nur mit Genehmigung des Ministeriums für Bildung, Jugend und Sport und mit Einwilligung der Erziehungsberechtigten durchgeführt werden. Darauf haben wir das anfragende Privatunternehmen hingewiesen und angeregt, dass den Erziehungsberechtigten zuerst eine Einsichtnahme in den Fragebogen ermöglicht wird, ehe sie ihre Einwilligung in die Umfrage erteilen, um so ihre umfassende Aufklärung sicherzustellen. Des Weiteren müssen die Schülerinnen und Schüler darüber aufgeklärt werden, dass ihre Teilnahme freiwillig ist. Darüber hinaus haben wir empfohlen, Schulkoordinatoren einzusetzen, die ohne Weisungsrecht gegenüber den Lehrkräften an der Schule dafür Sorge tragen, dass mit den im Zuge der Umfrageaktion erstellten Unterlagen datenschutzgerecht umgegangen wird.

Für die zur zweiten Stufe erforderliche Anschrift sollte ein vom Fragebogen getrenntes Extrablatt verwendet werden, da anderenfalls die Befragung nicht mehr anonym ist. Die Projektleitung sicherte zu, die Adressen der Interviewinteressenten in einem verschlossenen Umschlag weiter zu leiten. Die lediglich mit einem Code versehenen Fragebögen werden kuvertiert und mit dem Namen der Schule versehen zur Auswertung verschickt.

Schließlich haben wir empfohlen, im Anschreiben ausdrücklich auf die sichere Aufbewahrung der Daten und die Vernichtung sämtlicher Unterlagen spätestens nach Abschluss der Studie hinzuweisen. Die Vernichtung sollte protokolliert werden. Die Schule sollte die Einverständniserklärungen nur maximal drei Monate aufbewahren.

Die Gesellschaft hat unsere Hinweise berücksichtigt und in die Forschungsunterlagen aufgenommen. Nachdem das Ministerium das Projekt genehmigt hat, hängt dessen Durchführung jetzt von der Entscheidung der ausgewählten Schulen ab.

6.7 Internationale Schulleistungsstudie PISA - am datenschutzrechtlichen Fundament wird noch gearbeitet

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) betreibt das Internationale Forschungsprojekt PISA (Programme for International Student Assessment). PISA soll im drei Jahres Abstand die Leistungen 15-jähriger Schülerinnen und Schüler in den Bereichen Leseverständnis, Mathematik und Naturwissenschaften in rund 30 Industriestaaten evaluieren mit dem Ziel, den OECD-Mitgliedstaaten vergleichende Daten über die Leistungsfähigkeit ihrer Bildungssysteme zur Verfügung zu stellen. Die Bundesländer beteiligen sich nicht nur an PISA, sondern haben die Untersuchung um eine nationale Komponente unter Leitung des Max-Planck-Institutes erweitert.

In jedem Bundesland - so auch in Brandenburg - wurde zunächst eine Vorstudie in Form eines Feldtests an ausgewählten Schulen durchgeführt. Im März des vergangenen Jahres hat das Ministerium für Bildung, Jugend und Sport PISA genehmigt und uns erst danach die Forschungsunterlagen zur Verfügung gestellt. Wegen der aus datenschutzrechtlichen Gründen erforderlichen Verfahrenskorrekturen hat sich die Durchführung des Projekts verzögert.

Schon die Information der Erziehungsberechtigten im Rahmen der Vorstudie war unzureichend. Da die Probanden minderjährige Schülerinnen und Schüler sind, bedarf es einer schriftlichen Einwilligung der Erziehungsberechtigten, die wiederum eine umfassende Aufklärung über die geplanten Fragen voraussetzt. Hier hatten wir festgestellt, dass die Eltern nur unzulänglich über die Fragenkomplexe informiert wurden, die ihren Kindern gestellt werden sollten. Zwar wurden die Erziehungsberechtigten in einem Anschreiben auf die Aspekte hingewiesen, die sich aus dem Ziel der Studie ergeben, nicht jedoch auf die ebenfalls vorgesehenen Fragen nach dem persönlichen Umfeld oder auffälligem Sozialverhalten (z.B. Erziehungsstil der Eltern und Straftaten der Kinder). Solche besonders tief in den Privatbereich eindringenden Fragen lassen nicht ohne weiteres einen Bezug zum Inhalt des Forschungsprojekts erkennen. Wir haben daher gefordert, das Anschreiben, das die Erziehungsberechtigten zusammen mit der Einwilligungserklärung erhalten, um die noch fehlenden Informationen zu ergänzen.

Die Schülerinnen und Schüler selbst waren ebenfalls nicht ausreichend informiert. So fehlte der Hinweis, dass die Einwilligung ihrer Eltern auch minderjährige Probanden nicht verpflichtet, an der Studie teilzunehmen. Die Eltern haben dem die Studie durchführenden Institut lediglich das Recht erteilt, Daten zu erheben. Damit ist das Recht der grundrechtsmündigen Minderjährigen nicht aufgehoben, über ihre Teilnahme selbst zu bestimmen.

Die Einwilligung der Erziehungsberechtigten hat Auswirkungen auf den Umfang der Datenerhebung. Die Zustimmung umfasst nur solche Daten, die zur Durchführung der Studie unbedingt erforderlich sind. Da sich die Evaluierung auf die Leistungen 15-jähriger Schülerinnen und Schüler beschränken soll, ist zur Auswahl des Probandenkreises lediglich das Geburtsjahr, nicht aber das genaue Geburtsdatum erforderlich, so dass diese Daten auch nicht an das die Untersuchung durchführende Max-Planck-Institut übermittelt werden dürfen.

Schließlich war noch die Aufbewahrung und spätere Behandlung der personenbezogenen Unterlagen, insbesondere der schriftlichen Einwilligungserklärungen zu regeln.

Unterdessen hat das Max-Planck-Institut uns darüber informiert, dass die im Frühjahr 2000 stattfindende Hauptuntersuchung der Studie mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt werden soll, um eine datenschutzgerechte Gestaltung des Vorhabens zu erreichen. Die Datenschutzbeauftragten haben folgende Forderungen erhoben:

- Der Vorschlag, im berufsbildenden Bereich auf aktive Einwilligungserklärungen der Schüler bzw. Eltern zu verzichten, ist nicht akzeptabel. Vielmehr soll das Anschreiben an die Eltern unmittelbar durch die Schule selbst versandt und nicht mehr über die Schüler an diese weitergeleitet werden.

- Im Anschreiben an die Eltern soll ein Hinweis auf die EDV-mäßige Verarbeitung sowie auf die Vernichtung erfolgen.

- Schulrückmeldungen dürfen nur auf Wunsch der betroffenen Schulen und nur für den internen Gebrauch erfolgen, soweit eine bestimmte Teilnehmerquote erreicht ist. Bei Sonderschulen sollen anstatt Lehrer dieser Schule sonderpädagogische Fachkräfte als Aufsicht führende Personen beauftragt werden, damit die Anonymität gewahrt bleibt.

- Die ausgefüllten Fragebögen des nationalen Teils werden auf CD-ROM gesichert. Diese CD wird drei Jahre aufbewahrt. Ein entsprechender Hinweis wird in dem Anschreiben an die Eltern erfolgen.

- Der internationale Fragebogen sieht die Erhebung des Geburtstages vor. Dies ist nach Auffassung des Max-Planck-Institutes wichtig für die Erfassung der Kinder, deren Einschulungsdatum nicht zum Monatsende in den jeweiligen Ländern liegt. Es sollte zunächst festgestellt werden, für welche Länder die Erfassung der Daten solcher Kinder erforderlich ist. Ziel sollte auf jeden Fall sein, auf die Erhebung des genauen Geburtsdatums zu verzichten.

Die Wissenschaftler wollen diese Forderungen in den jeweiligen Unterlagen berücksichtigen und den Datenschutzbeauftragten zur Verfügung stellen, damit sie Gelegenheit erhalten, zu den überarbeiteten Unterlagen Stellung zu nehmen.

Korrekturen an nicht datenschutzgerecht geplanten Verfahren führen zu Verzögerungen bei der Durchführung von Forschungsvorhaben, die durch eine rechtzeitige Beteiligung des Datenschutzbeauftragten vermieden werden können.

7 Wissenschaft, Forschung und Kultur

Neues Hochschulgesetz verabschiedet

Im Rahmen der Beratungen zur Novellierung des Brandenburgischen Hochschulgesetzes haben wir zur Anpassung des Gesetzentwurfes der Landesregierung an das neu gefasste Brandenburgische Datenschutzgesetz Änderungen vorgeschlagen, die Eingang in das am 26. Mai 1999 in Kraft getretene neue Hochschulgesetz gefunden haben[58].

Neu in das Gesetz aufgenommen wurden außerdem Regelungen zur Evaluation der Lehre, die der Qualitätsentwicklung und -sicherung dienen sollen. Während die Evaluation hochschulintern durchaus mit Bezug auf einzelne Lehrkräfte durchgeführt werden kann, dürfen personenbezogene Angaben nicht an externe Stellen wie den Landeshochschulrat oder sogar private Gutachterinnen und Gutachter übermittelt werden. Auch dürfen die Ergebnisse der Evaluation nicht in die Personalakte des betroffenen Lehrenden aufgenommen werden. Etwas anderes gilt nur dann, wenn der Dienstvorgesetzte im Einzelfall besondere Maßnahmen für erforderlich hält und die Evaluationsergebnisse zum Gegenstand eines konkreten dienstrechtlichen Verfahrens werden.

Darüber bestand im Gesetzgebungsverfahren Einigkeit mit dem Ministerium für Wissenschaft, Forschung und Kultur.

Ergebnisse der hochschulinternen Evaluation der Lehre dürfen nur dann in die Personalakte des betroffenen Lehrenden aufgenommen werden, wenn im Einzelfall dienstrechtliche Maßnahmen ergriffen werden sollen. Eine personenbezogene Übermittlung der Evaluationsergebnisse an externe Stellen scheidet aus.

8 Arbeit, Soziales, Gesundheit und Frauen

8.1 Arbeit

[58] GVBl. I, S. 130 ff.

Ein Fax von unbekanntem Wirtschaftsprüfer

Der Inhaber eines Handwerksbetriebs, der Zuschüsse vom Land erhalten hatte, beschwerte sich bei uns darüber, dass sich ein privater Wirtschaftsprüfer unter Vorlage einer Vollmacht des Ministeriums für Arbeit, Soziales, Gesundheit und Frauen per Telefax an seine Geschäftsadresse gewandt und gefordert hatte, ihm bestimmte Nachweise zur Prüfung der ordnungsgemäßen Verwendung der Fördermittel zu überlassen.

Wir gingen angesichts der eigenständigen Prüftätigkeit des Beauftragten von einer Funktionsübertragung an ihn aus. Haushaltsrechtliche Vorschriften lassen es ausdrücklich zu, für solche Aufgaben auch selbständige Wirtschaftsprüfer einzusetzen, sodass es zur Aufgabenerfüllung erforderlich ist und im öffentlichen Interesse liegt, einem Beauftragten die dafür notwendigen Daten zu überlassen. Wirtschaftsprüfer können nach Auskunft des Ministeriums je nach dem Umfang der Aufgabenübertragung mit hoheitlichen Rechten beliehen werden. Beliehene Unternehmen unterliegen nach § 2 Abs. 1 Brandenburgisches Datenschutzgesetz unserer Kontrolle, während sonstige private Unternehmen unter der datenschutzrechtlichen Aufsicht des Ministeriums des Innern stehen. Im konkreten Fall war keine Beleihung erfolgt, weshalb wir die Angelegenheit mit dem Ministerium des Innern abstimmten. Gemeinsam konnten wir dem Ministerium für Arbeit, Soziales, Gesundheit und Frauen Empfehlungen geben, wie durch zusätzliche Vertragsbestimmungen der Datenschutz beim beauftragten Wirtschaftsprüfer zu verbessern ist. Hierzu gehörte auch die vom Petenten angesprochene Problematik, dass zum Schutz personenbezogener Daten deren Übermittlung per Telefax grundsätzlich zu unterbleiben hat.

Das Ministerium konnte, weil zwischenzeitlich der Vertrag mit dem Wirtschaftsprüfer ausgelaufen war, Nachbesserungen im konkreten Fall nicht mehr vornehmen. Es sagte aber zu, die Hinweise in Zukunft aufgreifen zu wollen.

Werden im Rahmen einer Funktionsübertragung zulässigerweise Daten durch Wirtschaftsprüfer erhoben, so ist der Datenschutz dort durch vertragliche Auflagen sicherzustellen.

8.2 Soziales

8.2.1 Sozialämter

8.2.1.1 Ein Sozialamt will mehr über die Hilfeempfänger wissen

Ein Landkreis bat uns um datenschutzrechtliche Beratung zur geplanten Durchführung einer Strukturanalyse seiner Sozialhilfeempfänger mit Hilfe eines privaten Unternehmens. Während wir nach einer vorläufigen Beurteilung auf weitere Informationen des Landkreises warteten, die klären sollten, ob es sich um ein Planungsvorhaben des Landkreises handelte oder ob von einem Forschungsvorhaben des Unternehmens auszugehen sei, schloss der Landkreis den Vertrag und ließ ihn im Sommer 1998 auch gleich teilweise umsetzen.

Erst nachträglich erhielten wir ausreichende Informationen, um die Angelegenheit bewerten zu können. Ebenfalls erst im Nachhinein wurde die Kommunalaufsicht durch das Kreissozialamt informiert. Diese war jedoch nicht zuständig, vielmehr hätten die Sozialdaten zu Forschungszwecken nur nach Genehmigung durch das Ministerium für Arbeit, Soziales, Gesundheit und Frauen übermittelt (vgl. § 79 II SGB X) werden dürfen. Wenigstens für den zweiten Teil der Strukturanalyse im Jahre 1999 wurde die Zustimmung des Ministeriums eingeholt und den meisten unserer Bedenken durch Auflagen in der Genehmigung Rechnung getragen.

Das Kreissozialamt verzichtete schließlich darauf, Angaben zu Straßenname und Hausnummer sowie dem Tag der Geburt der Betroffenen im Erhebungsbogen vorzusehen. Damit konnte eine gewisse Anonymisierung der Fragebögen erreicht werden.

Durch Änderung des Vertrages mit dem beauftragten Unternehmen ließen sich die Wahrung des Datenschutzes, hier auch des Sozialgeheimnisses und der technisch-organisatorische Ablauf verbessern.

Entsprechend unserer Forderung konkretisierte der Landkreis die Strukturanalyse. Anfänglich war geplant gewesen, zunächst die Datenerhebung und Basisauswertung von der Firma aufgrund ihrer Erfahrungen durchführen zu lassen und erst anschließend Fragestellungen von Seiten des Landkreises vorzugeben. Diese Vorgehensweise kann dazu führen, dass in den Erhebungsbögen Daten aufgenommen werden, ohne dass feststeht, ob diese für die Analyse erforderlich sind. Mit der Konkretisierung wurden diese Bedenken ausgeräumt. Schon aus Kostengründen sollte schließlich vor jeder Datenerhebung Klarheit über deren Sinn und Zweck geschaffen werden.

Unsere Bedenken konnten allerdings in einigen Punkten nicht gänzlich ausgeräumt werden:

Es wäre deutlich datenschutzgerechter gewesen, mit der Strukturanalyse bis zur Einführung neuer Software in den Sozialämtern zu warten, weil dies eine EDV-mäßige Lieferung bereits anonymisierter Daten an die Firma ermöglicht hätte. Der Landkreis erklärte gegenüber dem Ministerium, dies sei aus finanziellen Gründen noch längere Zeit nicht möglich. Eine spätere Erfassung der Daten setze aber den zeitlichen Zusammenhang und die direkte Vergleichbarkeit mit der Datenerfassung 1998 aufs Spiel und stelle damit das ganze Projekt in Frage.

Bei der ebenfalls datenschutzgerechteren Variante, die Einwilligung der Betroffenen zu erbitten, rechnete der Landkreis mit Problemen beim Rücklauf der Erklärungsformulare oder gar mit der Verweigerung der Zustimmung durch die Hilfeempfänger. Die Einwilligung einzuholen ist aber nicht deswegen unzumutbar, weil dafür ein nicht unerheblicher Verwaltungsaufwand notwendig ist oder weil damit gerechnet wird, dass die Betroffenen nicht einverstanden wären. Diese Argumentation verkennt, dass es zum Wesen der Freiwilligkeit gehört, dass die Einwilligung auch verweigert werden kann, zumal die Sozialdaten zu den besonders schützenswerten Daten im Verwaltungsbereich zählen. Wenn das Kreissozialamt hierzu vortrug, dass keine schutzwürdigen Interessen der Betroffenen beeinträchtigt würden, weil die Daten anonymisiert würden, so ignorierte es, dass vor der Anonymisierung eine Einsichtnahme in die Sozialamtsakten durch Mitarbeiter der Firma erfolgte.

Ganz überwiegend sollten für das Vorhaben des Landkreises Daten erhoben werden, die von den Sozialämtern mindestens einmal jährlich zum Jahresende für eine Bundesstatistik bereitgestellt werden müssen. Durch den Verzicht auf etliche Angaben beim zweiten Teil der Strukturanalyse reduzierte sich der Unterschied zu den Angaben, die zur Bundesstatistik herangezogen werden, noch weiter. Für uns stellt sich deshalb die Frage, ob die wenigen zusätzlichen Daten nicht auch noch von den Ämtern bereitgestellt werden könnten. Der Landkreis wandte ein, eigene Kapazitäten nicht verwenden zu können.

Wir erfuhren, dass der Landkreis nunmehr auch eine Bürgerbefragung durch Abiturienten im Bereich des Sozial- und Jugendamtes plant, um Aussagen zur Beratungsqualität zu erhalten. Gegen derartige Befragungen zur "Kundenorientierung" auch in der öffentlichen Verwaltung ist zwar prinzipiell nichts einzuwenden. Wir haben uns aber nochmals deutlich dagegen ausgesprochen, externe Interviewer in diesen datenschutzrechtlich besonders heiklen Bereichen zu beschäftigen. Wichtig erschien uns auch ein ausdrücklicher Hinweis an die Bürger, dass die Beantwortung der Fragen freiwillig, also insbesondere von der Gewährung beantragter Sozialleistungen unabhängig ist. Auch ist zu beachten, dass bei der Befragung personenbezogene Daten der Beschäftigten erhoben werden und diesem datenschutzrechtlichen Aspekt Rechnung getragen werden muss.

Es ist ein legitimes Anliegen, wenn ein Sozialhilfeträger sich einen genaueren Überblick über die Struktur der Hilfeempfänger verschaffen will oder an Rückmeldungen zu seinem Service interessiert ist. Jedoch müssen die damit einhergehenden Datenerhebungen rechtlichen Grundsätzen genügen.

8.2.1.2 Häufig auftretende Probleme in Sozialämtern

Im Rahmen der in diesem Jahr vorgenommenen Schulungen zum Sozialdatenschutz bei den örtlichen Trägern der Sozialhilfe wurden uns immer wieder Fälle vorgetragen, in denen Rechtsanwälte Auskünfte vom Sozialamt begehrten oder dem Sozialamt Informationen lieferten.

1. *Ein Rechtsanwalt wollte die aktuelle Adresse eines Sozialhilfeempfängers erfahren, um im Scheidungsverfahren den Antragsgegner mit ladungsfähiger Anschrift angeben zu können. Eine zuvor erfolgte Anfrage beim Einwohnermeldeamt hatte nicht weitergeholfen.*

2. *Andere vertraten Gläubiger und baten das Sozialamt um Auskunft darüber, ob Betroffene, die angegeben hatten, von Sozialhilfe zu leben, dem Sozialamt auch tatsächlich bekannt seien.*

3. *Wieder andere trugen dem Sozialamt Umstände vor, die dort zu Zweifeln an der Hilfebedürftigkeit der Betroffenen führten und verlangten zugleich vom Sozialamt eine Rückmeldung über den Ermittlungsstand.*

Den Sozialämtern war zwar bewusst, dass in solchen Fällen keine Übermittlungsbefugnis in den Vorschriften des Sozialgesetzbuches vorgesehen ist. Dennoch ließen sie sich verunsichern.

1. Bei Fragen nach Adressen von Sozialhilfeempfängern gilt, dass Fragesteller zunächst an das Einwohnermeldeamt zu verweisen sind, weil dort die aktuellen Meldedaten vorhanden sein müssten und sich anders als bei einer entsprechenden Auskunft des Sozialamtes nicht indirekt ergibt, dass der Betroffene Sozialhilfeempfänger ist.

Brachte eine Anfrage bei der Meldebehörde kein Ergebnis, so kann für die Verfolgung von Unterhaltsansprüchen oder den Versorgungsausgleich eine Mitteilung von Sozialdaten nach § 74 Abs. 2 SGB X zulässig sein, wenn zuvor der Versuch unternommen wurde, diese Daten beim Betroffenen selbst zu erfragen. Für ein Schreiben an den Betroffenen darf das Sozialamt einem Auskunftsberechtigten die Anschrift mitteilen. Eine Übermittlungsbefugnis für Sozialdaten nur zum Zweck eines Scheidungsantrags besteht jedoch nicht. Eine ablehnende Antwort des Sozialamtes nehmen Anwälte möglicherweise jedoch ebenso gerne entgegen wie eine aussagekräftige Auskunft. Durch die Fehlanzeige des Einwohnermeldeamtes und die Ablehnung des Auskunftsersuchens durch das Sozialamt weisen sie nämlich den zuständigen Gerichten nach, dass sie alles ihnen Mögliche versucht haben, eine Bezeichnung des Antraggegners beizubringen, so dass dem Gericht nun eine öffentliche Zustellung der Klage möglich wird.

2. Eine Befugnis, einem privaten Gläubiger zu bestätigen, dass der Schuldner von Sozialhilfe lebt, besteht nicht. Vorsicht ist aber auch dann geboten, wenn der Schuldner dem Sozialamt nicht bekannt ist. Würde das Sozialamt

in solchen Fällen mitteilen, dass es die Person nicht kennt, stünde es in den Fällen, in denen Sozialhilfeempfänger benannt sind, vor dem Problem, welche Auskunft es nun erteilen sollte, damit die Anfragenden nicht schon aus der anders lautenden Antwort ihre Schlüsse ziehen. Wir haben in allen solchen Fällen eine neutrale Formulierung empfohlen, die beispielsweise lauten könnte: "Wir können Ihnen über die Adresse des Betreffenden nichts mitteilen. Damit ist jedoch nicht zwingend ausgeschlossen, dass uns seine Adresse bekannt ist und u. U. an andere Stellen offenbart werden dürfte."

3. Tragen Privatpersonen beim Sozialamt Umstände vor, die es veranlassen, eigene Ermittlungen über die Hilfebedürftigkeit der Betroffenen aufzunehmen, so ergibt sich daraus keine Übermittlungsbefugnis an die Hinweisgeber. Wiederholten Nachfragen solcher Personen sollte gleich von vornherein begegnet werden, indem diesen beispielsweise eine Eingangsbestätigung zugesandt wird, die zugleich den Hinweis enthält, dass das Sozialamt nicht befugt ist, mitzuteilen, ob und was es aufgrund des Hinweises unternimmt sowie zu welchem Ergebnis es in dem Fall kommt.

8.2.1.3 Einwilligung statt richterlicher Anordnung - einfallsreiche Anfragen an Sozialämter

Ein Sozialhilfeempfänger war in den Verdacht geraten, eine Straftat begangen zu haben. Im Rahmen dieses Ermittlungsverfahrens bat die Polizei das Sozialamt um Mitteilung darüber, ob und in welcher Höhe der Betroffene Sozialleistungen beziehe. Seinem Auskunftsersuchen fügte die zuständige Polizeidienststelle zugleich eine Einwilligungserklärung des Betroffenen für sämtliche Leistungsträger im Sozialleistungsbereich bei.

Wir konnten dem Sozialamt bestätigen, dass seine Bedenken, aufgrund dieser Einwilligungserklärung Auskünfte an die Polizei zu erteilen, zu Recht bestanden. Zwar ergab sich aus § 73 Abs. 2 SGB X eine Befugnis zur Übermittlung der nachgefragten Sozialdaten zur Durchführung eines Strafverfahrens wegen der konkreten Straftat, die Übermittlung hätte nach § 73 Abs. 3 SGB X aber vom Richter angeordnet sein müssen. Dieses besondere Formerfordernis kann nicht durch eine Erklärung des Betroffenen ersetzt werden. Als Beschuldigter im Strafverfahren steht er stets unter einem gewissen Druck, sodass die Freiwilligkeit seiner Einwilligungserklärung fraglich ist. Zudem wird mit dem gewählten Verfahren ein gesetzlich vorgegebener Weg umgangen.

Von einem anderen Sozialleistungsträger wurde uns eine ähnliche Vorgehensweise der Staatsanwaltschaft geschildert. Auch in diesem Fall berief sich die Staatsanwaltschaft zur Klärung einer strafrechtlichen Rehabilitationsangelegenheit auf eine Einwilligungserklärung des Betroffenen. Die Ermittlungen der Staatsanwaltschaft erfolgten in diesem Fall eher zu Gunsten des Betroffenen und im Auftrag des zuständigen

Gerichts. Eine spezielle Übermittlungsbefugnis hat das Sozialgesetzbuch für diese Konstellation nicht vorgesehen. Eine Übermittlung der für das Rehabilitationsverfahren erforderlichen Sozialdaten war daher nur aufgrund einer Einwilligungserklärung des Betroffenen möglich. Zudem bestehen in einem solchen Zusammenhang auch keine Zweifel an der Freiwilligkeit.

Sieht das Gesetz besondere Übermittlungsbefugnisse vor, so ist eine Einwilligungserklärung weder notwendig noch dürfen mit ihr gesetzliche Formerfordernisse umgangen werden. Ist die Übermittlung von Sozialdaten jedoch für die Auskunft begehrende Stelle erforderlich, ohne dass eine Rechtsvorschrift die Offenbarung von Sozialdaten an diese Stelle vorsieht, so kann sich eine Übermittlungsbefugnis allein aus der Einwilligungserklärung des Betroffenen ergeben, insbesondere wenn die Behörde zur Wahrung der Interessen des Betroffenen tätig wird.

8.2.2 Sozialversicherungsträger

8.2.2.1 Patientendaten für die Krankenhausplanung?

Ein Krankenhaus machte uns Mitte des Jahres darauf aufmerksam, dass in einzelnen seiner Fachabteilungen sämtliche Behandlungsfälle aus dem Jahre 1998 vom Medizinischen Dienst der Krankenversicherungen begutachtet werden sollten. Dieser Auftrag war von den Verbänden der Krankenkassen im Land erteilt worden. Hintergrund waren Standortfestlegungen, die Klärung von Patientenwanderungen in einzelnen Regionen und der Wunsch, eine Entscheidungsbasis für den Antrag eines anderen Krankenhauses über die Erhöhung seiner Bettenzahl zu erhalten.

Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hat sich von Anfang an uns gegenüber auf den Standpunkt gestellt, dass hierfür anonyme Angaben genügten. Der Medizinische Dienst hatte jedoch vorgesehen, Einsicht in die Originalunterlagen zu nehmen. In den Erhebungsbögen sollten nur Name, Vorname, Straße und Wohnort nicht genannt werden, sodass lediglich geringfügig anonymisierte Daten das Krankenhaus verlassen würden.

Der Medizinische Dienst wollte sich auf § 17 a Krankenhausfinanzierungsgesetz (KHG) i. V. m. § 275 Abs. 4 Fünftes Buch Sozialgesetzbuch (SGB V) stützen. Er führte aus, dass eine Fehlbelegung ausgeschlossen werden müsse und jeder Tag der Behandlung in jedem Fall medizinisch gerechtfertigt sein müsse.

Wir haben weder den von § 17 a KHG geforderten "gezielten Anlass" für die Fehlbelegungsprüfung gesehen, noch konnten wir akzeptieren, dass dieses Merkmal durch die Argumentation, dass eine Fehlbelegung generell ausgeschlossen sein müsse, umgangen wird.

Der Medizinische Dienst akzeptierte schließlich, dass er nur anonymisierte Unterlagen erhalten dürfe.

Zur Krankenhausplanung bedarf es keiner Sammlung patientenbezogener Daten.

8.2.2.2 Böse Überraschung auf dem Anrufbeantworter

Ein Petent gab im Antrag eines Sozialversicherungsträgers unter der Rubrik "Telefonisch tagsüber zu erreichen" seine geschäftliche Telefonnummer an, weil im einleitenden datenschutzrechtlichen Hinweis um vollständiges Ausfüllen des Formulars gebeten worden war. Unter dieser Rufnummer war zusätzlich ein Anrufbeantworter geschaltet, den auch die Mitarbeiter des Betroffenen abhörten. Obwohl bereits der Text des Anrufbeantworters deutlich zu erkennen gab, dass es sich um den Anrufbeantworter einer Firma handelte, hinterließ ein Mitarbeiter des Sozialversicherungsträgers, der eine Rückfrage zum Antrag des Betroffenen hatte, sensible Sozialdaten auf dem Band. Der Betroffene fand später eine Notiz eines Mitarbeiters über diese Nachricht auf seinem Schreibtisch.

Dies ist eine unzulässige Offenbarung von Sozialdaten an Dritte. Der betroffene Sozialversicherungsträger hat den Vorfall sehr bedauert und dem in seinem Recht auf Wahrung des Sozialgeheimnisses Verletzten ein Entschuldigungsschreiben zugeleitet. Der Sozialversicherungsträger hat vielfache Vorkehrungen getroffen, um einen solchen Fall in Zukunft zu vermeiden:

Alle Mitarbeiter werden ausdrücklich auf das Sozialgeheimnis verpflichtet. Insbesondere wurde erläutert, dass auf Anrufbeantwortern ausschließlich um Rückruf zu bitten ist und keinesfalls Angaben über den Grund der telefonischen Anfrage gemacht werden dürfen.

Keine Möglichkeit, unsere Empfehlungen umzusetzen, sah die betroffene Stelle dagegen bei der Formulargestaltung. Wir hatten klargestellt, dass nach § 67 a Abs. 3 SGB X der Betroffene auch darauf hinzuweisen ist, welche Angaben in den Antragsformularen freiwillig sind. Dies gilt insbesondere für die Angabe der Telefon- oder Telefax-Nummer. Aufgrund des einleitenden Hinweises zu dem Fragebogen, dass die Informationen benötigt würden und die gestellten Fragen vollständig beantwortet werden sollten, entsteht der falsche Eindruck, dass eine Verpflichtung besteht, die dienstliche Telefonnummer anzugeben. Man sieht sich jedoch außer Stande, unseren Hinweisen

Rechnung zu tragen, da die Anträge bundesweit einheitlich verwandt werden und der zuständige Bundesverband die Anregung nicht aufgreifen will.

Telefonate können zwar das Verfahren beschleunigen, der Schutz für dabei ausgetauschte personenbezogene Daten ist aber deutlich geringer als bei einer Beförderung von Nachrichten auf dem Postweg im verschlossenen Umschlag. Die Notwendigkeit telefonischer Kontaktaufnahmen ist daher sorgfältig zu prüfen. Nachrichten auf Anrufbeantwortern, selbst wenn es sich nur um die Bitte um einen Rückruf handelt, sollten vermieden werden. Über durch das Sozialgeheimnis geschützte Themen darf nur mit dem Betroffenen bzw. seinem Bevollmächtigten selbst gesprochen werden.

8.2.3 Sozialgerichte: Öffentliche Verhandlung kontra Sozialdatenschutz

Ein Rechtsbeistand hat sich bei uns darüber beschwert, dass die von den Sozialversicherungsträgern als vertraulich zu betrachtenden Daten bei einem Rechtsstreit vor dem Sozialgericht entgegen seinem Antrag öffentlich verhandelt wurden.

Hier kollidieren der Grundsatz der öffentlichen Gerichtsverfahren mit dem Recht des Datenschutzes. Personenbezogene Daten, die bei einem Sozialleistungsträger dem Sozialgeheimnis (§ 35 Abs. 1 SGB I) unterlagen, müssen von der Stelle, an die sie übermittelt worden sind, in demselben Umfang geheim gehalten werden wie von dem Sozialleistungsträger. Gerichte sind von dieser Regelung nicht ausgenommen. Personenbezogene Daten, die ein Betroffener bei Gericht selbst vorträgt, sind jedoch nicht in dieser Weise geschützt. Diese Gemengelage, aber auch die historisch bedingte Öffentlichkeit von Gerichtsverfahren, bei denen Entscheidungen ausdrücklich "im Namen des Volkes" ergehen, führt dazu, dass auch die Verfahren vor den Sozialgerichten öffentlich stattfinden.

Ob ausnahmsweise die Öffentlichkeit ausgeschlossen werden kann oder muss, entscheidet das Sozialgericht selbst. Wir sind wegen der richterlichen Unabhängigkeit nicht befugt, eine solche Entscheidung zu beanstanden.

Für den Petenten konnten wir daher nicht mehr tun, als die nicht einfach verständliche Rechtslage zu erläutern. Wir würden es aber begrüßen, wenn die Gerichte bei ihrer Entscheidung über einen Antrag auf Ausschluss der Öffentlichkeit das Recht auf informationelle Selbstbestimmung des Betroffenen mehr in den Vordergrund stellen. Die verfahrensbeteiligten Verwaltungen sollten Betroffene insoweit unterstützen[59].

[59] s. 3. Tätigkeitsbericht 1994, Pkt. 4.2.1

Bei jedem Rechtsstreit müssen die Beteiligten damit rechnen, dass der Schutz ihrer personenbezogenen Daten wegen der prinzipiellen Öffentlichkeit von Gerichtsverhandlungen eingeschränkt wird.

8.3 Gesundheit

8.3.1 Krankenhäuser: Neue Bestimmungen zum Datenschutz in Sicht

Die Landesregierung hatte sich bisher gegenüber unseren Änderungswünschen zur Krankenhaus-datenschutzverordnung[60] zurückhaltend gezeigt und sich darauf berufen, dass aus der Praxis dem zuständigen Ministerium noch nichts bekannt geworden sei, was auf einen akuten Regelungsbedarf schließen ließ. Im Laufe des vergangenen Jahres wurden jedoch praktische Probleme, für welche in den bisherigen Bestimmungen keine Lösungen zu finden sind, deutlich.

Zum einen hat sich als klärungsbedürftig erwiesen, was im Fall von Schließungen insbesondere privat getragener Kliniken mit den Krankenunterlagen geschehen soll, wenn der ehemalige Träger entweder nicht mehr existiert oder aus finanziellen Gründen nicht in der Lage ist, sich dieser Frage anzunehmen.

Zum anderen mussten wir feststellen, dass ein landeseigenes Krankenhaus einen externen privaten Datenschutzbeauftragten bestellt hatte. Dies wäre schon nach dem Brandenburgischen Datenschutzgesetz, wonach behördlicher Datenschutzbeauftragter nur ein Bediensteter der öffentlichen Verwaltung sein darf, unzulässig. Im Hinblick darauf, dass selbstständige Externe nicht als ärztliche Gehilfen angesehen werden können und der Bruch einer vertraglich vereinbarten Schweigepflicht nicht nach § 203 Strafgesetzbuch (StGB) mit Strafe bedroht ist, ist es nicht tragbar, an sie Patientendaten zu offenbaren.

Aufgrund dieser ungelösten Probleme sieht das zuständige Ministerium unterdessen einen Regelungsbedarf. Es neigt auch dazu, den Datenschutz in stationären Einrichtungen im Landeskrankenhausgesetz selbst zu regeln. Dies hielten wir im Hinblick darauf, dass Eingriffe in das Recht auf informationelle Selbstbestimmung und Befugnisse zur Durchbrechung der ärztlichen Schweigepflicht in Rede stehen, von Anfang an für erforderlich. Auch bietet das die Chance, die Widersprüche zwischen Vorschriften der Krankenhausdatenschutzverordnung und des Brandenburgischen Archivgesetzes eindeutig zu Gunsten des Patientendatenschutzes zu klären.

---

[60] s. Tätigkeitsbericht 1998, Pkt. 7.3.1

Über diesen sowie weiteren Regelungs- bzw. Klarstellungsbedarf aus unserer praktischen Erfahrung mit der Krankenhausdatenschutzverordnung haben wir das Ministerium vor kurzem informiert und ihm unsere Unterstützung angeboten.

8.3.2 Gesundheitsämter

8.3.2.1 Organisationsprüfer wollen Amtsärzten über die Schulter sehen

Ein mit der Durchführung von Organisationsuntersuchungen betrauter Mitarbeiter des Hauptamtes wollte an schulärztlichen Reihenuntersuchungen des Gesundheitsamtes teilnehmen, um den Zeitaufwand und die Effektivität der Vorgehensweise der Ärzte besser beurteilen zu können. Der Amtsarzt wehrte sich dagegen unter Hinweis auf den Datenschutz und die ärztliche Schweigepflicht und hob hervor, dass auch die personenbezogenen Daten von Kindern diesem Schutz unterlägen.

Das Gesundheitsamt ist bei der Verarbeitung von Daten grundsätzlich an die ärztliche Schweigepflicht gebunden. Eine Einschränkung der ärztlichen Schweigepflicht wäre nur für den Fall denkbar, dass konkrete Anhaltspunkte für ein Verhalten von Mitarbeitern des Gesundheitsamtes vorliegen, das arbeits- oder strafrechtliche Konsequenzen nach sich ziehen könnte. Hier wären die Ärzte zur Wahrung ihrer Interessen darauf angewiesen, nähere Umstände aus dem Arzt-Patienten-Verhältnis mitzuteilen. Solche konkreten Anhaltspunkte liegen jedoch bei Beginn einer bloßen Organisationsuntersuchung regelmäßig nicht vor. Sie muss sich daher zunächst auf nicht patientenbezogene Angaben beschränken. Der zuständige behördliche Datenschutzbeauftragte hatte vorgeschlagen, dass das jeweilige Fachamt entsprechendes anonymisiertes Zahlenmaterial beizubringen habe. Erst dann, wenn sich hieraus konkreter Klärungsbedarf ergibt, der zu einem arbeits- oder dienstrechtlichen Vorverfahren führt, ist ein Mitarbeiter des Gesundheitsamtes berechtigt, zu seiner Entlastung patientenbezogene Daten aufzudecken.

Die vom Hauptamt zunächst geplante Teilnahme an amtsärztlichen Untersuchungen wäre mit der ärztlichen Schweigepflicht keinesfalls zu vereinbaren. Diese von allen denkbaren Maßnahmen am meisten beeinträchtigende Verfahrensweise ist zudem weder erforderlich noch zumutbar. Dementsprechend darf auch nicht versucht werden, diese Vorgehensweise mit Hilfe einer Einwilligungserklärung der Patienten bzw. ihrer Erziehungsberechtigten zu ermöglichen.

Für den Fall, dass sich eine Akteneinsicht in Behandlungsunterlagen durch die Organisationsuntersucher schließlich als unverzichtbar erweisen sollte, haben wir unter Hinweis auf einen Beschluss des Bundesverfassungsgerichts zur Rechnungsprüfung in einem Krankenhaus auf weitere Anforderungen hingewiesen: Die Beziehungen zwischen Prüfern und betroffenen Patienten müssen anonym sein. Dies erfordert es, sicherzustellen, dass die Prüfer die betrof-

fenen Patienten nicht kennen. Außerdem müssen die Prüfer ihrerseits besonders zur Verschwiegenheit verpflichtet werden. Die Prüfberichte selbst dürfen nur anonymisierte Daten enthalten.

8.3.2.2 Zu viel der Fürsorge: Amtsarzt informiert den Personalrat

Eine Petentin, Angestellte im öffentlichen Dienst, wurde von ihrem Arbeitgeber zum Amtsarzt geschickt, um ihre Dienstfähigkeit beurteilen zu lassen. Mit ihrer Zustimmung zog der Arzt des Gesundheitsamtes weitere Befunde ihrer behandelnden Ärzte hinzu. Die Betroffene machte deutlich, dass diese Angaben ihrem Arbeitgeber nicht bekannt gegeben werden sollten. Dies sicherte das Gesundheitsamt ihr zu und vereinbarte darüber hinaus, das Gutachten zunächst mit der Betroffenen zu besprechen, bevor es dem Arbeitgeber bekannt gegeben würde. Letztlich hat das Gesundheitsamt den öffentlichen Arbeitgeber jedoch ohne Rücksprache mit der Betroffenen über das Ergebnis des Gutachtens informiert. Dies führte zu einer krankheitsbedingten Kündigung, gegen welche die Betroffene Klage erhob. In dem gerichtlichen Verfahren wies der Arbeitgeber darauf hin, dass das Gesundheitsamt in einem Gespräch dem Personalrat und der Schwerbehindertenvertretung das Gutachten erläutert habe. Mithin seien die angesprochenen Stellen umfassend informiert gewesen, obwohl die Betroffene dem Personalrat die Akteneinsicht in ihre Personalakte, in der das Gutachten verwahrt werde, nicht gestattet habe.

Wir haben der Betroffenen erläutert, dass das Gesundheitsamt nach § 29 Abs. 2 Nr. 2 Brandenburgisches Gesundheitsdienstgesetz (BbgGDG) i. V. m. § 18 BbgGDG befugt sei, ihrem Arbeitgeber als Auftraggeber des amtlichen Gutachtens dessen Ergebnis mitzuteilen. Nach Darstellung des Amtes waren dabei keine medizinischen Daten offenbart worden, die von anderen Ärzten stammten. Wir konnten auch nicht feststellen, dass das Gesundheitsamt hierbei den Erforderlichkeitsgrundsatz verletzt hätte. Vielmehr war es dem Amtsarzt ein Anliegen, darzustellen, dass dem Arbeitgeber keine Diagnosen mitgeteilt würden, sondern Erkrankungen so allgemein wie möglich umschrieben würden. Im Wesentlichen ging es ihm darum, die gesundheitlichen Einschränkungen darzustellen und Empfehlungen zur Einsatzfähigkeit der Begutachteten zu geben.

Seine Befugnisse überschritten hat das Gesundheitsamt aber damit, dass es Informationen über das Gutachtenverfahren an den Personalrat und die Schwerbehindertenvertretung offenbarte. Der Amtsarzt als Leiter des Gesundheitsamtes hat eingeräumt, dass ein solches Gespräch nicht hätte erfolgen dürfen. Er nahm daher den Fall zum Anlass, eine grundsätzliche Belehrung aller Ärzte seines Amtes zu Auskünften über Begutachtete, Gestaltung von Gutachten und rechtliche Konsequenzen von Verstößen gegen Offenbarungspflichten durchzuführen.

Wegen des Auskunftsrechts der Betroffenen über die zu ihrer Person gespeicherten Daten und deren Verwendung, also auch die Offenbarung an Dritte, hätte zudem die Besprechung des Gesundheitsamtes mit dem Personalrat und der Schwerbehindertenvertretung in der Patientenakte dokumentiert werden müssen.

9 Wirtschaft

9.1 Datenschutz und öffentliche Fördermittel

Ein Petent war von der Investitionsbank des Landes Brandenburg aufgefordert worden, die ihm bereits gewährten Fördermittel zurückzuzahlen. Ihr Vorgehen begründete die Bank mit erheblichen Bedenken an der persönlichen Zuverlässigkeit des Petenten, da ihr unterdessen ein Ermittlungsverfahren gegen den Petenten wegen des Verdachts, er verbreite Propagandamittel verfassungswidriger Organisationen, bekannt geworden war. Die Staatsanwaltschaft hatte das Ermittlungsverfahren allerdings bereits wieder eingestellt, nachdem weder Hausdurchsuchungen noch Postbeschlagnahme genügend Anhaltspunkte erbracht hatten, um Anklage zu erheben.

9.1.1 Übermittlungen von Erkenntnissen durch die Verfassungsschutzbehörde

Die Prüfung ergab, dass nicht nur - wie der Petent vermutet hatte - die Staatsanwaltschaft, sondern in erster Linie die Brandenburgische Verfassungsschutzbehörde ihre Erkenntnisse über den Petenten weitergegeben hatte. Anlass für die Übermittlung war ein Ersuchen des Ministeriums für Wirtschaft, Mittelstand und Technologie, an das sich die Investitionsbank gewandt hatte, nachdem sie einer Presseveröffentlichung Anhaltspunkte entnommen hatte, der Petent gehöre dem rechtsextremen Spektrum an. Bei der Informationsweitergabe an das Wirtschaftsministerium stützt sich die Verfassungsschutzbehörde auf § 16 Abs. 1 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG), wonach sie personenbezogene Daten an inländische Behörden übermitteln darf, wenn dies zur Erfüllung ihrer (d. h. der Verfassungsschutzbehörde) Aufgaben erforderlich ist. Der brandenburgische Gesetzgeber hat die Verfassungsschutzbehörde zusätzlich zu der Aufgabe, Informationen über verfassungsschutzrelevante Bestrebungen zu sammeln, auch beauftragt, die Landesregierung und andere zuständige Stellen über Gefahren für die freiheitliche demokratische Grundordnung zu unterrichten (§ 1 Abs. 2 BbgVerfSchG).
Die Prüfung der bei der Verfassungsschutzbehörde vorhandenen Unterlagen über den Petenten ergab, dass die Informationen den gesetzlichen Vorgaben gemäß erhoben und gespeichert worden sind. Bei der Übermittlung der Erkenntnisse an das Wirtschaftsministerium handelte es sich um einen Einzelfall, der aufgrund der besonderen Gefahrenlage auch datenschutzrechtlich hingenommen werden kann.

9.1.2 Akteneinsicht der Investitionsbank bei der Staatsanwaltschaft

Nachdem das Wirtschaftsministerium vom Verfassungsschutz auch über das Ermittlungsverfahren gegen den Petenten informiert worden war, hat die Investitionsbank Akteneinsicht bei der Staatsanwaltschaft beantragt. Diese wurde ihr nach den Richtlinien für das Straf- und Bußgeldverfahren gewährt. Danach ist die Akteneinsicht zulässig, wenn die Behörden ein berechtigtes Interesse darlegen, das die schutzwürdigen Belange der Betroffenen überwiegt. Da das Verfahren gegen den Petenten gem. § 170 Abs. 2 Strafprozessordnung eingestellt worden war, weil die Ermittlungen den Anfangsverdacht nicht bestätigt hatten, konnte die Staatsanwaltschaft in diesem Fall sogar davon ausgehen, mit der Gewährung der Akteneinsicht im Interesse des Petenten zu handeln, zumal die Investitionsbank bereits von dem Ermittlungsverfahren wusste.

Datenerhebung und -nutzung durch die Investitionsbank

Die Investitionsbank gewährt Finanzierungshilfen auf der Grundlage der Landeshaushaltsordnung sowie weiterer Gesetze und Verwaltungsvorschriften, wenn die Prüfung ergeben hat, dass das Land ein erhebliches Interesse an der Gründung bzw. Fortführung eines Unternehmens hat. Dabei darf die Finanzierungshilfe nur solchen Empfängern gewährt werden, bei denen eine ordnungsgemäße Geschäftsführung gesichert erscheint und die in der Lage sind, die Verwendung der Mittel bestimmungsgemäß nachzuweisen. Daraus leitet die Investitionsbank die Verpflichtung ab, die Zuverlässigkeit des Zuwendungsempfängers sowohl in persönlicher als auch in finanzieller Hinsicht zu prüfen. Aus den Vorschriften geht jedoch nicht hervor, bis in welche Lebensbereiche und bis zu welcher Tiefe eine solche "Zuverlässigkeitsprüfung" vorgenommen werden darf. Insbesondere kann auch der Antragsteller nicht ersehen, dass die Investitionsbank zur Überprüfung seiner Angaben ggf. bei anderen Stellen nachfragt. Für eine über den Bonitätsrahmen hinausgehende Prüfung durch die Landesinvestitionsbank gibt es keine Rechtsgrundlage.

Da die Gewährung von Finanzierungshilfen bundesweit einheitlich gehandhabt wird, müsste auch die Erweiterung der Zuverlässigkeitsprüfung bundeseinheitlich geregelt werden. Wir haben daher das Wirtschaftsministerium aufgefordert, sich für eine entsprechende bundesweite Regelung einzusetzen.

Zur Frage, inwieweit politische Überzeugungen von Antragstellern bei der Vergabe von Subventionen im Rahmen der Zuverlässigkeitsprüfungen eine Rolle spielen dürfen oder ob diese Prüfung sich auf die Bonität und strafrechtlichen Ermittlungen oder Verurteilungen zu beschränken hat, ist gegenwärtig ein Verwaltungsstreitverfahren anhängig.

Schon jetzt aber müssten die Betroffenen vor der Beantragung solcher Finanzierungshilfen wissen, dass sie durch ihren Antrag eine umfassende Zuverlässigkeitsprüfung ihrer Person auslösen können. Gerade wegen der weitreichenden Konsequenzen, die mit der Inanspruchnahme von Finanzierungshilfen verbunden sind, muss der Antragsteller umfassend informiert sein, um die ausgelösten Überprüfungen und Datenflüsse überblicken zu können.

9.2 Auch Schornsteinfeger haben Stillschweigen zu wahren

Einen Petenten verließ das Vertrauen in seinen zuständigen Bezirksschornsteinfegermeister. Dieser hatte an den Bauträger des Hauses, welches der Petent nun sein Eigen nannte, die Information weitergegeben, dass der Petent beabsichtigt, eine zweite Heizungsanlage zu installieren.

Die Weitergabe der Information an den Bauträger stellt eine unzulässige Datenübermittlung im Sinne des Schornsteinfegergesetzes (SchfG) dar. Danach darf der Bezirksschornsteinfegermeister personenbezogene Daten an nicht-öffentliche Stellen nur übermitteln (§ 19 Abs. 4 SchfG), soweit der Empfänger ein rechtliches Interesse an der Kenntnis der Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Dieser hat in seiner Funktion als Bezirksschornsteinfegermeister, der mit der Wahrnehmung öffentlicher Aufgaben betraut und daher Beliehener ist, von dem Bauvorhaben Kenntnis erlangt. Der Petent war nach § 42 Abs. 10 Brandenburgische Bauordnung nämlich verpflichtet, sich vom Bezirksschornsteinfegermeister vor Inbetriebnahme einer Feuerungsanlage das Vorliegen bestimmter Eignungsvoraussetzungen schriftlich bescheinigen zu lassen.

Die Kenntnis von dem Bauvorhaben hat der Bezirksschornsteinfegermeister an eine nicht-öffentliche Stelle, nämlich den Bauträger als juristische Person des Privatrechts weitergegeben, obwohl dieser die Daten weder angefordert, noch ein rechtliches Interesse an ihrer Kenntnis glaubhaft dargelegt hatte.

Auch Bezirksschornsteinfegermeister dürfen personenbezogene Daten an nicht-öffentliche Stellen nur übermitteln, soweit diese ein rechtliches Interesse an der Kenntnis der Daten glaubhaft darlegen und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

10 Landwirtschaft, Umweltschutz und Raumordnung

10.1 Europäischer Gerichtshof stärkt den Zugang zu Umweltinformationen

Der Europäische Gerichtshof erklärte in seinem Urteil vom 9. September 1999[61] mehrere Regelungen des deutschen Umweltinformationsgesetzes für nicht mit dem Gemeinschaftsrecht[62] vereinbar. Diese Entscheidung hat auch Auswirkungen auf die Rechte der Bürgerinnen und Bürger des Landes Brandenburg sowie die brandenburgischen Verwaltungen.

Der Gerichtshof stellte fest, dass das Umweltinformationsgesetz keine ausdrückliche Bestimmung über die auszugsweise Übermittlung von Umweltdaten enthält, und schließt daraus, dass in Deutschland die Pflicht zur auszugsweisen Übermittlung von Informationen über die Umwelt nicht so klar gewährleistet ist, dass die Rechtssicherheit ausreichend garantiert ist. Personen, die einen Antrag auf Informationen über die Umwelt stellen wollen, sollen von allen ihren Rechten - so auch der Möglichkeit auf eine auszugsweise Übermittlung - Kenntnis erlangen können.
Darüber hinaus urteilte der Gerichtshof, dass der vollständige Ausschluss des Rechts auf Einsicht in Umweltdaten für die Zeit eines Verfahrens, das die angefragten Daten zum Gegenstand hat, über den im Gemeinschaftsrecht geregelten Ausnahmetatbestand hinausgeht. Eine Beschränkung von umweltbezogenen Informationsrechten sei in einem Verwaltungsverfahren danach nur möglich, wenn es einem gerichtlichen oder quasigerichtlichen Verfahren unmittelbar vorausgeht und durchgeführt wird, um Beweise zu beschaffen oder ein Ermittlungsverfahren durchzuführen.

Weiter sorgt der Gerichtshof für eine Entlastung der Portmonees der Bürgerinnen und Bürger für den Fall, dass ihr Antrag auf Zugang zu Umweltinformationen abgelehnt wird. Das Umweltinformationsgesetz gestattete bisher die Erhebung einer Gebühr selbst im Fall der Ablehnung eines Informationsersuchens. Diese Bestimmung hält der Gerichtshof für nicht mit der Richtlinie vereinbar. Sie könnte einzelne Bürgerinnen und Bürger davon abhalten, einen Antrag auf Informationen zu stellen.

---

[61] *Rs C-217/97, DVBl. 1999, S. 1494 ff.*

[62] *Richtlinie des Rates vom 07.06.1990 über den freien Zugang zu Informationen über die Umwelt (90/313/EWG), ABl EG Nr. L 158 S. 56*

Das Land Brandenburg steht nun in der Pflicht, seine Verwaltungsvorschriften zum Vollzug des Umweltinformationsgesetzes an das Urteil des Gerichtshofes anzupassen. Gleiches gilt für die Umweltinformationsgebührenordnung, die zur Zeit noch die Festsetzung von Gebühren auch bei ablehnenden Bescheiden zulässt. Auch für die noch anstehende Gebührenordnung zum Akteneinsichts- und Informationszugangsgesetz hat diese Rechtsprechung Konsequenzen[63].

10.2 Rechtsanwaltsgebühren als Geschäftsgeheimnis?

Der Minister für Ernährung, Landwirtschaft und Forsten hat auf die Kleine Anfrage eines Abgeordneten, die auf die Höhe der Kosten zur Anfertigung eines außergerichtlichen Gutachtens gerichtet war, geantwortet, dass die Gebühren aufgrund der Bundesgebührenordnung für Rechtsanwälte entstanden sind. Der Minister meinte jedoch, der konkrete Betrag unterliege als Geschäftsgeheimnis dem Datenschutz[64].

Diese Auffassung teilen wir nicht. Nicht alles, was der Geheimhaltung unterliegt, lässt sich unter den Datenschutz subsumieren. Dieser soll nur die rechtmäßige Verarbeitung der Daten natürlicher Personen sichern (vgl. § 1 Bundesdatenschutzgesetz, § 1 Brandenburgisches Datenschutzgesetz). Ein Geschäftsgeheimnis dagegen ist i. d. R. kein personenbezogenes Datum, sondern jede auf ein Geschäft oder einen Betrieb bezogene Tatsache, die nur ein begrenzter Personenkreis kennt, die der Geschäfts- oder Betriebsinhaber erkennbar und berechtigt geheim halten will und die anderen Personen nicht ohne Weiteres zugänglich sind. Der Verrat von Betriebsgeheimnissen kann nach § 19 des Gesetzes gegen den unlauteren Wettbewerb strafbar sein und nach den Vorschriften des Bürgerlichen Gesetzbuches zum Schadensersatz verpflichten. Datenschutzrechtliche Vorschriften kommen nicht zur Anwendung.

Wir hatten aber auch erhebliche Zweifel, ob der genaue Betrag des Rechtsanwaltshonorars, dessen Mindestniveau aus der Bundesrechtsanwaltsgebührenordnung abgeleitet werden kann, als Betriebs- und Geschäftsgeheimnis qualifiziert werden kann. Insbesondere schien uns kein überwiegendes privates Interesse im Sinne des Artikels 56 Abs. 4 der Landesverfassung vorzuliegen, das eine Geheimhaltung dieses Betrages zwingend erfordert. Vielmehr überwiegt das Interesse des Abgeordneten, von der Landesregierung Auskunft über die Mittelverwendung einer landeseigenen Gesellschaft zu erhalten.

In diesem Zusammenhang haben wir darauf hingewiesen, künftig auch unter dem Gesichtspunkt des Artikels 56 der Verfassung des Landes Brandenburg genau zu prüfen, inwieweit Daten überhaupt der Geheimhaltung unterliegen

---

63 s. unten B 2.3

64 *Kleine Anfrage Nr. 2002, LT-Drs. 2/6443*

und insbesondere personenbezogene Daten geschützt werden müssen. Wenn Datenschutz lediglich als Vorwand benutzt wird, so birgt dies die Gefahr in sich, dass das Ziel, die Wahrung des informationellen Selbstbestimmungsrechts, verkannt wird. Gerade dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht ist daran gelegen, dem vorzubeugen. Das Ministerium für Ernährung, Landwirtschaft und Forsten hat auf unser Schreiben hin eingeräumt, dass die Geheimhaltung von Geschäftsgeheimnissen kein Datenschutzproblem darstellt.

Betriebs- und Geschäftsgeheimnisse unterliegen in aller Regel nicht dem Datenschutz, sondern anderen gesetzlichen Bestimmungen. Die Verweigerung von Auskünften an Abgeordnete rechtfertigen sie nur dann, wenn das überwiegende Interesse an ihrer Geheimhaltung dies zwingend erfordert.

11 Stadtentwicklung, Wohnen und Verkehr

11.1 "Identitätsklau" und Behördenschlamperei

Ein Petent hat uns gebeten, dafür Sorge zu tragen, dass die anlässlich eines gegen ihn geführten Ermittlungsverfahrens erhobenen Daten aus einer erkennungsdienstlichen Behandlung und einer DNA-Analyse gelöscht werden. Bei der Bearbeitung seiner Eingabe stellte sich heraus, dass der Petent Opfer eines durch Behördenschlamperei ermöglichten sog. Identitätsdiebstahls geworden war, bei dem der ihm vor Jahren zusammen mit seinem Personalausweis gestohlene Führerschein verwendet wurde. Unsere Anfragen bei Polizei, Staatsanwaltschaft und Führerscheinstellen führten nicht nur zur Vernichtung der Unterlagen, sondern vor allem auch zur überfälligen Korrektur des Führerscheinregisters.

Im Berichtszeitraum war der Fahrer eines in Schlangenlinien durch die Stadt fahrenden Pkw's, von einer Funkstreife angehalten und wegen des Verdachts der Trunkenheit am Steuer zur Wache gebracht worden. Nach einem Alkoholtest, der den Verdacht bestätigte, wurde dem Fahrer der Führerschein entzogen und er selbst mit dem Verweis, dass er nicht mehr Auto fahren dürfe, entlassen. Die Polizeibeamten beobachteten jedoch, dass der Fahrer sich wieder an das Steuer seines unmittelbar vor der Wache geparkten Fahrzeugs setzte und davon fuhr. Eine unverzüglich alarmierte Einsatzstreife stellte den Fahrer in einer anderen Stadt, konfrontierte ihn mit den Tatvorwürfen der Trunkenheit am Steuer und des Fahrens ohne Führerschein. Zurück in die Wache gebracht, wurde ein weiterer Blutalkoholtest vorgenommen. Eine Überprüfung seiner Personalien mittels Personalausweis sowie ein Abgleich der Daten des entzogenen Führerscheins mit dem INPOL-Fahndungsbestand (Informationssystem der Polizei) wurde nicht durchgeführt.

Als dem Fahrer der Anhörungsbogen zugeschickt wurde, kam das Schreiben mit dem Vermerk "Unbekannt" zurück. Von der Meldestelle erhielt die Polizei Name und Anschrift des Petenten und stellte ihm den Anhörungsbogen zu. Dessen Einwände, dass er die in Rede stehenden alkoholumnebelten Fahrten nicht unternommen habe und dafür auch Zeugen benennen könne, blieben unbeachtet. Obwohl er dem Anhörungsbogen zum Beweis, dass sein Führerschein nicht beschlagnahmt worden sei, eine Kopie seines Führerscheins beifügte, wurde er weiterhin als Tatverdächtiger betrachtet und schließlich als Beschuldigter vor Gericht gestellt. Erst das Amtsgericht versuchte seine Einlassungen aufzuklären, indem es mehrmals die vollständige Führerscheinakte des Petenten anforderte. Die zuständige Führerscheinstelle teilte jedoch mit, dass es keine Akte gebe und schickte lediglich Registerauszüge. Schließlich ordnete das Amtsgericht eine Blutentnahme bei dem Petenten und die anschließende DNA-Analyse (sog. genetischer Fingerabdruck) der Blutprobe an, um durch den Abgleich mit den seinerzeit entnommenen Blutproben festzustellen, ob der Petent mit dem damaligen Fahrer identisch sei. Der Abgleich ergab, dass die Blutproben von unterschiedlichen Personen stammten und der Petent somit unschuldig war. Das Verfahren wurde eingestellt.

Die erkennungsdienstlichen Unterlagen sowie die Ergebnisse der DNA-Analyse, die sich immer noch in den Ermittlungsakten der Staatsanwaltschaft bzw. in den Akten des mit der Analyse beauftragten Instituts befanden, wurden erst im Zuge der durch die Eingabe des Petenten ausgelösten erneuten Bearbeitung der staatsanwaltschaftlichen Akten vernichtet. Erst danach wurden auch die Eintragungen im Führerscheinregister sowie in der Akte berichtigt.

Rechtsgrundlage für die Blutentnahme ist § 81 a Strafprozessordnung (StPO), dem gemäß eine körperliche Untersuchung des Beschuldigten zur Feststellung von Tatsachen angeordnet werden kann, die für das Verfahren von Bedeutung sind. Dazu dürfen auch Blutproben gegen den Willen des Betroffenen entnommen werden, wenn kein Nachteil für seine Gesundheit zu befürchten ist. Um festzustellen, ob Spurenmaterial von dem Beschuldigten stammt, dürfen die Blutproben molekulargenetisch untersucht werden. Wenn es zur Erforschung der Wahrheit erforderlich ist, können sogar die ohne ihre Einwilligung entnommenen Blutproben anderer Personen als den Beschuldigten einer DNA-Analyse unterzogen werden (§ 81 c und e StPO). Maßnahmen, die auf der Grundlage der Strafprozessordnung angeordnet werden, müssen dem allgemeinen Verhältnismäßigkeitsgrundsatz genügen. DNA-Analysen unterliegen demnach keinen anderen gesetzlichen Beschränkungen als die übrigen Identifizierungsinstrumente im Strafverfahren. Wenn die Untersuchungsergebnisse vorliegen und ausgewertet sind, müssen die Blutproben und dazugehörigen Unterlagen vernichtet werden (§ 81 a Abs. 3 StPO).

Da es sich in diesem Fall um schwerwiegende Verstöße gegen die Straßenverkehrsordnung handelte, konnte das Verfahren nicht als Verfahren gegen Unbekannt eingestellt werden, solange nicht alle Mittel ausgeschöpft waren, um festzustellen, ob der Petent nicht doch mit dem Beschuldigten identisch ist. Anhand des Führerscheins und des

dazugehörigen Registerauszuges sah sich das Gericht zu dieser Entscheidung nicht in der Lage. Der Führerschein war ein untaugliches Beweismittel, weil aus den Führerscheinregistereintragungen nicht hervorging, dass ein anderer als der Petent die auf ihn ausgestellten Führerscheine nutzte. Die Blutentnahme und anschließende DNA-Analyse war also rechtlich zulässig.

Dennoch bleibt es unbefriedigend, dass aufgrund der Schlamperei mehrerer Behörden in so schwerwiegender Weise in die Grundrechte eines Unschuldigen eingegriffen worden ist. Schon durch die einfache polizeiliche Standardmaßnahme einer ordnungsgemäßen Personalienüberprüfung einschließlich Abfrage der Personalausweisdaten im INPOL-Fahndungssystem, in dem u. a. alle abhanden gekommenen Personalausweise mit Seriennummer registriert sind, wäre es überhaupt nicht zur Verwechslung des Petenten mit dem Fahrer gekommen. Stattdessen wurden die Ermittlungen so nachlässig fortgeführt, wie sie begonnen worden waren. So hat die Polizei offensichtlich die vom Petenten zu Beginn des Ermittlungsverfahrens zur Verfügung gestellte Kopie seines Führerscheins nicht mit dem beschlagnahmten Führerschein verglichen, sonst hätte ihr nämlich auffallen müssen, dass sich Foto, Ausstellungsdatum und Führerschein-Nummern der beiden Dokumente voneinander unterschieden und daher die Prüfung, ob hier ein Diebstahl vorlag, geboten war.

Ebenso nachlässig hat die zuständige Führerscheinstelle gearbeitet. Dort ist anscheinend vergessen worden, dem Kraftfahrtbundesamt mitzuteilen, dass der Petent einen neuen Führerschein erhalten hatte und der alte Führerschein ungültig war mit der Folge, dass zu beiden Führerscheinen nur eine Registereintragung auf den Namen des Petenten existierte. Der Datensatz des Petenten im Führerscheinregister wurde erst im Zuge der Bearbeitung seiner Eingabe berichtigt. Ebenso schlampig ist die zweimalige Anforderung des Amtsgerichts, die Führerscheinakte zu übersenden, bearbeitet worden. Statt der Akte, in der die Verlustmeldung des gestohlenen Führerscheins und die Neuausstellung dokumentiert sind, wurden lediglich nicht aussagefähige Registerauszüge übersandt.

Behördenschlamperei kann zu Grundrechtseingriffen bis hin zu Eingriffen in die körperliche Unversehrtheit bei Bürgerinnen und Bürgern führen, die bei korrekter Aufgabenerfüllung der Verwaltung zu vermeiden gewesen wären.

11.2 Befragung von Wohnungseigentümern durch private Gutachter

Das Ministerium für Stadtentwicklung, Wohnen und Verkehr hat einen externen Dritten mit der Erstellung eines Gutachtens über die "Wirtschaftlichkeit und Entwicklungsperspektiven vermieteter Altbaubestände im Eigentum von Privatpersonen" beauftragt. Wir wurden gebeten, datenschutzfreundliche Möglichkeiten zu benennen, wie der Beauftragte Namen und Anschriften der Eigentümer erhalten könnte.

Das Ministerium stellte drei Alternativen zur Diskussion: Telefonbefragungen, Versendung von Fragebögen durch die Grundsteuerstellen und Versendung von Fragebögen durch die Katasterämter. Von Telefonbefragungen raten wir dringend ab, da eine ausreichende Vertraulichkeit und Dokumentation nur schwer sichergestellt werden kann.

Das Verfahren der Versendung von Fragebögen durch Grundsteuerstellen können wir nur bedingt empfehlen. Die Grundsteuerstellen sind zur Wahrung des Steuergeheimnisses verpflichtet (§ 30 Abgabenordnung). Aus diesem Grund besteht lediglich die Möglichkeit, über das Adressmittlungsverfahren die Versendung der Fragebögen vorzunehmen. Dabei ist darauf zu achten, dass die Grundsteuerstelle auf dem zu versendenden Briefumschlag zunächst ihren eigenen Absender vermerkt, damit, wenn der Empfänger nicht bekannt ist und der Brief an den Absender zurückgeleitet wird, ausgeschlossen wird, dass der Gutachter als externer Dritter die Adresse zur Kenntnis bekommt. Die Grundsteuerstelle würde dagegen nur ihre "eigenen" Daten zurückbekommen. Mit dem Adressmittlungsverfahren bleibt der Zweckbindungsgrundsatz (vgl. § 13 BbgDSG) gewahrt. Zwar werden die Daten (hier die Adressen) nicht für den bei der Erhebung bestimmten Zweck genutzt. Da jedoch keine Übermittlung an Dritte stattfindet, die Daten verarbeitende Behörde also die Daten nur nutzt, halten wir dieses Verfahren für vertretbar. Durch das Adressmittlungsverfahren wird die Nutzung personenbezogener Daten auf das Minimalmaß beschränkt. Schutzwürdige Interessen der betroffenen Bürger werden nicht beeinträchtigt.

Wir hätten allerdings einer Versendung der Fragebögen durch die Katasterämter den Vorzug gegeben, die nach dem Vermessungs- und Liegenschaftsgesetz möglich gewesen wäre und nicht den Umweg eines Adressmittlungsverfahrens verlangt.

Das Ministerium hat sich demgegenüber für das Verfahren der Versendung von Fragebögen durch die Grundsteuerstellen mittels Adressmittlung entschieden. Dazu hat es mit dem Auftragnehmer einen Werkvertrag geschlossen, in dem in Folge unserer Intervention die datenschutzrechtlichen Anforderungen über die Datenverarbeitung im Auftrag (§ 11 BbgDSG) festgeschrieben wurden.

11.3 Versäumte Aufklärung von Häuslebauern

Im Zuge der Überprüfung unterer Bauaufsichtsbehörden mussten wir wiederholt feststellen, dass Bauantragstellerinnen und Bauantragsteller über die Verarbeitung ihrer Daten während des Baugenehmigungsverfahrens nicht aufgeklärt wurden. Eine Behörde war der Meinung, der Aufklärungspflicht nicht nachkommen zu müssen. Das Ministerium für Stadtentwicklung, Wohnen und Verkehr zog sogar unsere Befugnis zur Überprüfung unterer Bauaufsichtsbehörden in Zweifel.

Trotz der ausdrücklichen Verpflichtung (§ 12 Abs. 3 Satz 2 BbgDSG) zur Aufklärung der Betroffenen über den Zweck der Datenerhebung, die beabsichtigte Art der Weiterverarbeitung sowie den Empfängerkreis bei einer beabsichtigten Datenübermittlung, unterblieb dies in den unteren Bauaufsichtsbehörden. Wir haben den überprüften Stellen empfohlen, die Betroffenen spätestens dann aufzuklären, wenn Dritte im Verfahren eingeschaltet werden. Darüber hinaus würde eine nachträgliche Unterrichtung, welchen Behörden und sonstigen Stellen die personenbezogenen Daten übermittelt wurden, dem Zweck des § 12 Abs. 3 Satz 2 BbgDSG nicht gerecht werden, so dass die Aufklärung im bauaufsichtlichen Verfahren, wenn überhaupt, nur im Rahmen der Antragstellung möglich wäre. Als vorerst zweckmäßigste Lösung haben wir die Erweiterung der Eingangsbestätigung für den Bauantrag oder die Aushändigung eines separaten Merkblattes empfohlen und dafür einen entsprechenden Vorschlag unterbreitet.

In den unteren Bauaufsichtsbehörden wird nun bis auf eine Ausnahme die Aufklärung über die Datenverarbeitung im bauaufsichtlichen Verfahren vorgenommen. Die untere Bauaufsichtsbehörde einer kreisfreien Stadt ist jedoch der Auffassung, dass § 12 Abs. 3 Satz 2 BbgDSG wegen des Vorrangs der datenschutzrechtlichen Vorschriften des § 91 der Brandenburgischen Bauordnung (BbgBO) nicht anwendbar sei. Dem war zu entgegnen, dass § 91 Abs. 6 BbgBO uneingeschränkt auf die Anwendung des Brandenburgischen Datenschutzgesetzes verweist, soweit keine spezialgesetzliche Regelung getroffen wurde. Da die Brandenburgische Bauordnung keine speziellen Regelungen über die Aufklärungspflicht bei beabsichtigten Datenübermittlungen enthält, kommt § 12 BbgDSG ergänzend neben § 91 BbgBO zur Anwendung. Darüber hinaus haben wir mitgeteilt, dass mit der Aufklärung spätestens dann zu beginnen ist, wenn Dritte im Verfahren eingeschaltet werden. Die untere Bauaufsichtsbehörde hat den Zeitpunkt der Aufklärung der Betroffenen so früh wie möglich zu wählen, gerade auch um dem Zweck des § 12 Abs. 3 Satz 2 BbgDSG gerecht zu werden, d. h. den Bauantragsteller darüber zu informieren, welche Datenverarbeitungsmaßnahmen beabsichtigt sind.

Ihrer gesetzlichen Aufklärungspflicht nach dem Datenschutzgesetz können sich die Bauaufsichtsbehörden auch nicht unter Hinweis auf die Bauvorlagenverordnung und die gegenwärtige Fassung der Antragsformulare entziehen.

Da aufgrund der von uns durchgeführten Kontrollen zu vermuten ist, dass eine weitere Zahl von Bauämtern ihrer Aufklärungspflicht nach § 12 Abs. 3 BbgDSG nicht nachkommt, haben wir das Ministerium gebeten, dafür Sorge zu tragen, dass die unteren Bauaufsichtsbehörden als selbständige Daten verarbeitende Stellen die Bestimmungen des Brandenburgischen Datenschutzgesetzes und andere Bestimmungen über den Datenschutz einzuhalten haben. Eine optimale und frühestmögliche Aufklärung der Betroffenen wäre dabei tatsächlich im Rahmen der Bauantragstellung zu erreichen, was einer Änderung der Bauvorlagenverordnung bzw. der entsprechenden Verwaltungsvorschrift bedürfte.

Das Ministerium hat sich dazu bisher nicht positioniert, vorab jedoch die Kontrollbefugnis des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht bezweifelt, in dem es die Auffassung vertritt, das Brandenburgische Datenschutzgesetz sehe eine unmittelbare Kontrollbefugnis des Landesbeauftragten gegenüber den Gemeinden und Gemeindeverbänden bei der Wahrnehmung bauaufsichtlicher Aufgaben nicht vor.

Dies verkennt die Rechtslage. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat nach § 23 Abs. 1 BbgDSG gegenüber den in § 2 Abs. 1 BbgDSG genannten öffentlichen Stellen ein umfassendes Kontrollrecht. Öffentliche Stellen im Land Brandenburg unterliegen nur insoweit nicht oder mit Einschränkungen der Kontrolle durch den Landesbeauftragten, als sie in § 2 Abs. 1 a und Abs. 2 BbgDSG genannt sind. Untere Bauaufsichtsbehörden sind die Landkreise, die kreisfreien Städte und die großen kreisangehörigen Städte und damit Gemeinden und Gemeindeverbände i. S. v. § 2 Abs. 1 Satz 1 BbgDSG. In datenschutzrechtlicher Hinsicht sind sie sowohl als öffentliche als auch als Daten verarbeitende Stellen anzusehen. Auch die unteren Bauaufsichtsbehörden unterstehen uneingeschränkt den datenschutzrechtlichen Vorschriften und unterliegen damit den Kontroll- und Beratungsbefugnissen des Landesbeauftragten.

Untere Bauaufsichtsbehörden haben als selbständige Daten verarbeitende Stellen die Bauantragstellerinnen und Bauantragsteller über die beabsichtigte Verarbeitung ihrer Bauantragsdaten gem. § 12 Abs. 3 BbgDSG aufzuklären.

12 Finanzen

12.1 Zugriff des Finanzamts auf die Computer der Steuerpflichtigen?

Die von Steuerpflichtigen gefürchtete Betriebsprüfung ist bislang im Wesentlichen darauf angewiesen, sich mit den Akten und Papieren eines Betriebes auseinanderzusetzen. Das wird als eine Art Wettbewerbsnachteil der Steuerfahndung angesehen, der nunmehr durch Änderungen der gesetzlichen Grundlagen der Außenprüfung behoben werden soll.

Exemplarisch ist hierfür die vorgeschlagene Neuregelung des § 147 der Abgabenordnung (AO): Danach soll den Finanzbehörden im Rahmen der Außenprüfung u. a. das Recht eingeräumt werden, die Datenverarbeitungssysteme der Steuerpflichtigen zu nutzen, die diese zur Erstellung ihrer den Finanzbehörden vorgelegten Unterlagen benutzt haben und in die betreffenden Dateien Einsicht zu nehmen. Prinzipiell wird man dieses Bestreben angesichts der Einbeziehung neuer Techniken zur Erstellung von Unterlagen unterstützen müssen. Doch darf daraus keine Erweiterung von Eingriffsbefugnissen gegenüber der bisherigen papiergestützten Praxis folgen. Der Zugang zur

EDV darf allerdings nicht dazu genutzt werden, selbst eigenständige Recherchen in den Dateien der Steuerpflichtigen vorzunehmen. Nach der geltenden Rechtslage sind die Steuerpflichtigen nämlich verpflichtet, die einschlägigen Unterlagen selbst vorzulegen. Erst, wenn sie der entsprechenden Aufforderung der Finanzbehörden nicht nachkommen, hat letztere die Möglichkeit, in einem besonderen, rechtsstaatlich ausgeformten Verfahren Verwaltungszwang auszuüben. Durch die Gewährung eines beliebigen Zugangs zu Datenverarbeitungssystemen der Steuerpflichtigen könnten diese klaren Grenzen staatlicher Zugriffsmöglichkeit verschwimmen.

Im Rahmen des noch andauernden Gesetzgebungsverfahren gelang es teilweise, diesen Aspekt in die Beratungen einzubringen: So soll der Zugriff auf die Datenverarbeitungssysteme nur auf das elektronische Pendant der vorzulegenden papierenen Unterlagen beschränkt werden und keine unbeschränkte Recherchemöglichkeit in diesem Stadium des Verfahrens, welches noch keine auch unter strafrechtlichen Gesichtspunkten zu betrachtende Steuerfahndungsmaßnahme darstellt, eröffnen. Ferner wird nicht - wie am Anfang des Gesetzgebungsprozesses gefordert - den Finanzbehörden einen Online-Zugriff ermöglicht. Dennoch bedarf es noch einer weiteren Konkretisierung einzelner Elemente der vorgesehenen Regelungen, damit die Grenzen der Befugnisse der Finanzbehörden deutlicher werden. Wir werden auch den weiteren Gesetzgebungsprozess kritisch begleiten.

Darüber hinaus steht jedoch die notwendige Ergänzung der Abgabenordnung um bereichsspezifische Regelungen für eine datenschutzgerechte Gestaltung des Besteuerungsverfahrens aus. Die obersten Finanzbehörden des Bundes und der Länder lehnen es ab, die Vorschläge der Datenschutzbeauftragten aufzugreifen. Stattdessen wird die Abgabenordnung - wie das Beispiels des § 147 zeigt - nach Art eines Flickenteppichs um Regelungen zur Datenverarbeitung nur dort ergänzt, wo es den Interessen der Finanzbehörden dient. Dabei besteht kein Zweifel, dass in mehreren, die Steuerpflichtigen direkt berührenden Bereichen wie den Auskunfts- und Akteneinsichtsrechten, Löschungsregelungen, Rahmenbedingungen für das Outsourcing und Datenexport dringender Novellierungsbedarf besteht, auch um den Vorgaben der EG-Datenschutzrichtlinie zu genügen.

Die Abgabenordnung muss dringend um bereichsspezifische Regelungen zum Datenschutz (Auskunfts- und Akteneinsichtsrechte, Löschungspflichten, Bedingungen für das Outsourcing, Datenexport) ergänzt werden.

12.2 Manchmal genügt ein kleiner Aufdruck zur Sicherung der Vertraulichkeit

Das Land Brandenburg ist zur sparsamen Mittelbewirtschaftung verpflichtet. Aus diesem Grund werden die Lohnsteuerkarten der Bediensteten des Landes bei ihrer Rückgabe an diese durch die Zentrale Bezügestelle

nicht über die Deutsche Post portopflichtig an die Privatanschrift versandt, sondern per portofreier Behördenpost an die Dienstanschrift.

In der Vergangenheit erfolgte dieses zwar in einem verschlossenen Umschlag, doch war er nicht als "vertraulich" oder "persönlich" gekennzeichnet. Ohne eine solche ausdrückliche Kennzeichnung gelangen Sendungen jedoch in den normalen Postgang der Verwaltung, mit der Folge, dass die Briefumschläge geöffnet wurden und so die Empfängerinnen und Empfänger erreichten. Zumindest jede mit der Zustellung der Behördenpost betraute Person, hätte nunmehr die Eintragungen auf den Lohnsteuerkarten lesen können.

Dabei handelt es sich neben der Anschrift, Angaben zum Familienstand und der Religionszugehörigkeit insbesondere um Angaben zum erzielten Jahreseinkommen und den abgeführten Steuern, mithin alles vertrauliche personenbezogene Informationen, die zudem auch noch durch das Steuergeheimnis einem besonderen Schutz unterliegen. Ein offener Versand oder eine Offenbarung an beliebige Dritte ist daher unzulässig und zu unterbinden. Dazu gehört auch die Verpflichtung, eine unbefugte Öffnung von Briefen nach Möglichkeit zu verhindern.

Aufgrund einer Eingabe wiesen wir die Zentrale Bezügestelle auf diese Problematik hin. Sie sicherte uns zu, künftig beim Versand von Lohnsteuerkarten mittels Behördenpost die verschlossenen Umschläge mit dem Aufdruck "vertraulich" zu versehen, so dass sichergestellt ist, dass die Sendung nur durch die Adressaten selbst geöffnet werden darf.

Vertrauliche Schreiben, die die Adressaten persönlich und nicht in ihrer dienstlichen Funktion betreffen, müssen ausdrücklich als "persönlich" oder "vertraulich" gekennzeichnet werden, damit sie nicht unzulässigerweise im normalen Dienstbetrieb geöffnet werden.

Teil B

Akteneinsicht und Informationszugang

Das Brandenburgische Akteneinsichts- und Informationszugangsgesetz ist seit zwei Jahren in Kraft und hat in dem Maße Auswirkungen auf die Praxis der Verwaltungsbehörden des Landes und der Gemeinden und Gemeindeverbände, in dem Bürgerinnen und Bürger sich auf dieses Gesetz berufen. Das bisher in der Bundesrepublik einmalige Akteneinsichts- und Informationszugangsgesetz hat aber auch über Brandenburg hinaus im Berichtszeitraum Wirkungen gezeigt. Zunächst sind die Entwicklungen auf europäischer Ebene zu skizzieren, die das Informationszugangsrecht in Deutschland und in Brandenburg beeinflussen werden.

1 Entwicklung des Informationszugangsrechts in Europa und Deutschland

1.1 Europa

Mit ihrem Grünbuch über die Informationen des öffentlichen Sektors in der Informationsgesellschaft ("Informationen des öffentlichen Sektors - eine Schlüsselressource für Europa")[65] hat die Europäische Kommission eine unionsweite Diskussion über eine Erweiterung der Zugangsrechte zu öffentlichen Informationen eröffnet. Auch wenn das Grünbuch einen Schwerpunkt auf die kommerzielle Nutzung der Informationen legt, hebt es doch zugleich die Bedeutung des Informationszugangsrechts der Unionsbürgerinnen und -bürger für die Unterstützung des demokratischen Prozesses hervor.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat zu den von der Kommission gestellten Fragen Stellung genommen[66] und dabei insbesondere folgende Punkte hervorgehoben:

1. Die Entwicklung des Internets hat die Möglichkeiten des Informationszugangs für alle erheblich verbessert und wird sie auch bezogen auf Informationen der öffentlichen Verwaltung weiter verbessern, wenn die Zahl der privaten Internetanschlüsse und der öffentlichen Kiosk-Terminals zunimmt. Selbst wenn das Internet für alle zugänglich sein sollte, darf es aber keine Kanalisierung des Informationszugangs auf die neuen Medien und erst recht keinen "Anschluss- und Benutzungszwang" geben. Der elektronische Zugriff kann nur eine zusätzliche - sicherlich immer wichtiger werdende - Kommunikationsmöglichkeit sein. Die Zugangsmöglichkeiten für Bürgerinnen und Bürger zu Informationen der öffentlichen Verwaltung dürfen aber nicht davon abhängig

---

65 KOM (98) 585 endg.; Ratsdok. 5580/99

66 s. Anlage 2

gemacht werden, dass ein Mindestmaß an entsprechendem technischen Know-how und Technikausstattung bei denjenigen vorhanden ist, die informiert werden wollen. Es muss möglich bleiben, persönlich im Rathaus oder in einer anderen Behörde Einsicht in eine (konventionelle oder elektronische) Akte zu nehmen.

2. Die Europäische Kommission sollte die notwendigen Schritte zur Rechtsangleichung auf europäischer Ebene durch Erarbeitung eines entsprechenden Richtlinienentwurfs unternehmen, um die unterschiedlichen Bedingungen des Informationszugangs in der Bundesrepublik und in der gesamten Europäischen Union sobald wie möglich zu harmonisieren.

3. Die Bereitstellung von Informationen über die bei der öffentlichen Verwaltung verfügbaren Daten, z. B. durch die Veröffentlichung von Aktenplänen und Datenbankstrukturen, ist eine wichtige Voraussetzung, um den Informationszugang zu erleichtern.

4. Die Kosten der Informationsbereitstellung und des Informationszugangs dürfen nicht insgesamt auf die Bürgerinnen und Bürger abgewälzt werden, die an den Informationen interessiert sind. Entsprechend dem Brandenburgischen Informationszugangsgesetz sollten die Gebühren so bemessen werden, dass zwischen dem Verwaltungsaufwand einerseits und dem Recht auf Akteneinsicht andererseits ein angemessenes Verhältnis besteht. Eine Differenzierung der "Preise" bzw. Gebühren danach, ob die gewünschten Informationen zur Wahrnehmung der demokratischen Rechte "wesentliche Bedeutung" haben oder nicht, erscheint problematisch. Zum einen würde es dem Grundanliegen jeder allgemeinen Informationszugangsgesetzgebung widersprechen, eine Begründung des Informationsinteresses zu verlangen, um danach bei Anerkennung eines "demokratischen Interesses" niedrige Gebühren, bei der Verfolgung rein kommerzieller Interessen dagegen entsprechend höhere Gebühren zu verlangen. Zum anderen müsste bei einer entsprechend differenzierten Gebührenstruktur auch das Problem gelöst werden, dass Informationen zunächst für einen "preiswerten" Zweck abgefragt und anschließend für einen "teueren" (kommerziellen) Zweck verwendet werden können.

5. Gewisse Formulierungen im Grünbuch deuten darauf hin, dass dem Datenschutz im Verhältnis zum Informationszugangsrecht von Unternehmen, die z. B. im Bereich der Direktwerbung tätig sind und deshalb in erster Linie an personenbezogenen Informationen interessiert sind, bisher ein zu geringer Stellenwert eingeräumt wird. Nach dem Brandenburgischen Akteneinsichts- und Informationszugangsgesetz kann das kommerzielle Verwertungsinteresse von Unternehmen den Schutz der Privatsphäre nicht zurückdrängen oder aufheben. Generell sind in der Bundesrepublik Eingriffe in das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger nur im überwiegenden Interesse der Allgemeinheit und nicht einzelner Unternehmen zulässig. Besonderen Stellenwert hat der Schutz der Privatsphäre beim Zugang zu sensiblen personenbezogenen Daten wie den medizinischen Informationen sowie Arbeitnehmer- und Sozialdaten.

Auch wenn - mit Einwilligung der Betroffenen - personenbezogene Daten im Rahmen der Akteneinsicht Dritten zugänglich gemacht worden sind, so werden sie dem Anwendungsbereich der Datenschutzgesetze damit nicht entzogen. Die bisher angestellten Überlegungen zur Verzahnung des Datenschutzes und des allgemeinen Informationszugangsrechts bedürfen noch der Präzisierung. Ein massenhafter Abruf personenbezogener Daten, z. B. für Zwecke der Direktwerbung, ist z. B. in Kanada mit seiner längeren Tradition des Informationszugangsrechts nicht zulässig; er sollte auch in der Europäischen Union nicht ermöglicht werden. Technische Beschränkungen des Informationszugangs wie z. B. Recherche-Restriktionen können unter Umständen den Schutz der Privatsphäre mit den Informationsinteressen der Allgemeinheit in Einklang bringen.

6. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat sich in seiner Stellungnahme dafür ausgesprochen, auch auf europäischer Ebene eine gemeinsame Kontroll- und Beratungsinstanz für Fragen des allgemeinen Informationszugangs und des Datenschutzes entsprechend dem Vorbild der meisten kanadischen Provinzen, Ungarns und des Landes Brandenburg zu schaffen.

Die Diskussion über das Grünbuch der Europäischen Kommission mit den einzelnen Stellungnahmen kann im Internet verfolgt werden[67].

Mit seinem Beschluss vom 17. Dezember 1999 zur Verbesserung der Information über die Gesetzgebungstätigkeit des Rates und das öffentliche Register der Ratsdokumente hat der Rat der Europäischen Union im Vorgriff auf die nach Art. 255 des Vertrages von Amsterdam festzulegenden Transparenzgrundsätze seine Absicht bekundet, die eigene Gesetzgebungstätigkeit transparenter zu gestalten. Dazu sollen die Tagesordnungen des Rates und der vorbereitenden Gremien, soweit sie Gesetzgebungsverfahren betreffen, mit Verweisen auf diesbezügliche Dokumente veröffentlicht werden.

Das seit dem 1. Januar 1999 über das Internet[68] zugängliche Register der Ratsdokumente soll Verweise auf die Dokumenten-Nummern und den Betreff von Verschluss-Sachen enthalten, soweit dem nicht der Schutz des öffentlichen Interesses, der Privatsphäre des Einzelnen, des Geschäfts- und Industriegeheimnisses, der finanziellen

---

67 http://www.echo.lu/legal/en/access.html

68 http://ue.eu.int

Interessen der Gemeinschaft oder nationale Rechtsvorschriften entgegenstehen. Bereits veröffentlichte Dokumente sollen spätestens am 1. Juli 2000 im Register angegeben und über das Internet zugänglich gemacht werden. Der Rat hat diesen - noch sehr allgemein und restriktiv gehaltenen - Beschluss vor dem Hintergrund gefasst, dass "Offenheit für demokratische Verhältnisse in der Europäischen Union und für ihre politische Verantwortlichkeit von entscheidender Bedeutung" ist "und die Unterrichtung der Öffentlichkeit eines der Instrumente zur Förderung dieser Offenheit" ist.

1.2 Bundesrepublik Deutschland

In der Bundesrepublik macht das Brandenburger Beispiel des Akteneinsichts- und Informationszugangsgesetzes zunehmend Schule. Sowohl im Nachbarland Berlin[69] als auch in Schleswig-Holstein[70] sind inzwischen Informationsfreiheitsgesetze beschlossen worden und in Kraft getreten. Deren Regelungen weichen im Detail vom Brandenburgischen Akteneinsichts- und Informationszugangsgesetz (AIG) ab. Gemeinsam ist allen diesen Gesetzen aber der Grundsatz, dass jede Person ohne Angabe von Gründen Zugang zu den bei einer Behörde vorhandenen Informationen verlangen kann. Wie in Brandenburg können Personen, die sich in ihren Rechten auf Informationszugang beeinträchtigt sehen, den jeweiligen Landesbeauftragten für den Datenschutz anrufen. Damit ist bereits in drei Bundesländern der Grundsatz des Allgemeinen Informationszugangs zu Unterlagen der öffentlichen Verwaltung mit Gesetzeskraft versehen worden. In Brandenburg hat er über die Regelung des Art. 11 der Landesverfassung sogar Grundrechtsqualität. Zugleich ist die Kontrolle des Informationszugangs mit der Datenschutzkontrolle vereinigt worden. Die Entscheidung über die sich überschneidenden Materien liegen so in einer Hand und können aufeinander abgestimmt werden.

---

[69] GVBl. Berlin 1999, S. 561 f.

[70] Gesetz über die Freiheit des Zugangs zu Informationen für das Land Schleswig-Holstein i. d. Fassung vom 26.1.2000

Die Informationsfreiheitsgesetze Berlins und Schleswig-Holsteins eröffnen auch zu personenbezogenen Daten zum Teil einen weiter gehenden Zugang der Öffentlichkeit, als dies in Brandenburg bisher zulässig ist. Auch begnügen sich diese Informationszugangsgesetze der zweiten Generation mit weniger Ausnahmen als das Brandenburgische Gesetz. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird in diesem Jahr aufgrund seiner bisherigen Erfahrungen mit der Anwendung des Akteneinsichts- und Informationszugangsgesetzes Vorschläge zur Novellierung dieses Gesetzes vorlegen[71], die die weiter gehenden Informationsfreiheitsgesetze in den beiden anderen Bundesländern berücksichtigen werden.

Die Bundesregierung verfolgt zwar entsprechend der Koalitionsvereinbarung von 1998 weiterhin das Ziel, ein Informationsfreiheitsgesetz für die Bundesebene bis zum Ende der Legislaturperiode zu verwirklichen[72], hat aber bisher keinen entsprechenden Gesetzentwurf vorgelegt.

Das Bundesverfassungsgericht hat im Dezember 1999 eine Grundsatzentscheidung gefällt, die zwar vordergründig nur den Rechtsschutz bei Sicherheitsüberprüfungen betrifft, aber auch erhebliche Auswirkungen bei der gerichtlichen Geltendmachung von Ansprüchen nach dem Akteneinsichts- und Informationszugangsgesetz haben wird[73]. Im konkreten Fall verlangte der Kläger, der seinen Arbeitsplatz in Folge einer negativen Auskunft des Verfassungsschutzes im Zuge der Sicherheitsüberprüfung verloren hatte, Offenlegung der zu Grunde liegenden Information, was der Verfassungsschutz nicht nur ihm, sondern auch dem angerufenen Verwaltungsgericht verwehrte. Dabei konnte sich die Behörde auf die Verwaltungsgerichtsordnung berufen, die eine unvollständige Aktenvorlage an das Gericht ausnahmsweise dann zulässt, wenn das Bekanntwerden der Akten dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen.

Das Bundesverfassungsgericht hat in dieser gesetzlichen Vorschrift und ihrer Anwendung einen Eingriff in das Grundrecht auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG) gesehen und den Gesetzgeber aufgefordert, die Verwaltungsgerichtsordnung entsprechend zu ändern. In der Tat stand bisher jeder, der seinen Anspruch auf Auskunft über die zu seiner Person vorhandenen Daten gerichtlich durchsetzen wollte und dem dieser "Staatswohlklausel" entgegen gehalten wurde, vor einem kafkaesken Dilemma: Die Behörde konnte einwenden, dass im Rechtsstreit über die Auskunftserteilung mit der Übergabe der gewünschten Information an das Gericht bereits die Rechtsfrage zu Gunsten des Klägers entschieden worden wäre, über die das Gericht erst befinden sollte. Aufgrund der Öffentlichkeit des Verfahrens hätte der Kläger schon vor der Entscheidung des Gerichts Zugang zu

---

71 vgl. schon Tätigkeitsbericht 1998, B 1.3.1

72 So der Staatssekretär im Bundesministerium, Schapper, beim Internationalen Symposium "Informationsfreiheit und Datenschutz" am 25.10.1999 in Potsdam

73 BVerfG, Beschluss vom 27.10.1999 - 1 BvR 385/90 -

den Informationen gehabt, die ihm nach Auffassung der Behörde zu Recht verweigert werden sollten. Das Bundesverfassungsgericht hat dieses Dilemma in der Weise gelöst, dass im Interesse eines effektiven Rechtsschutzes die Öffentlichkeit des Verfahrens in einem sog. "in-camera-Verfahren" in der Weise eingeschränkt wird, dass die streitigen Unterlagen zunächst nur dem Vorsitzenden des erkennenden Gerichts zugeleitet werden, der seinerseits über die Geheimhaltungsbedürftigkeit entscheidet, ohne dass der Kläger in diesem Stadium schon Zugang zu den Informationen erhält.

Dieses wegen der Entscheidung des Bundesverfassungsgerichtes bereits jetzt bundesweit in allen Verwaltungsgerichtsprozessen anzuwendende Verfahren ist auch zu beachten, wenn Personen in Brandenburg ihr Grundrecht auf Akteneinsicht gerichtlich gegen eine Behörde durchsetzen wollen, die sich auf eine der zahlreichen Ausnahmebestimmungen des Gesetzes beruft. In allen diesen Fällen kann das Dilemma einer vorweggenommenen Offenbarung der Information nur durch ein "in-camera-Verfahren" gelöst werden. Die Verwaltung ist dann nicht berechtigt, den Verwaltungsgerichten die vollständige Vorlage der Akten zu verweigern.
Wenden sich Bürgerinnen und Bürger - vor einer Anrufung der Verwaltungsgerichte - dagegen an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, so hat dieser ohnehin ein vollständiges Einsichtsrecht in die Verwaltungsunterlagen. Wenn im Einzelfall das zuständige Mitglied der Landesregierung feststellt, dass die Einsicht in die Unterlagen die Sicherheit des Bundes oder eines Landes gefährdet, so hat die Landesregierung auf Antrag des Landesbeauftragten dies im zuständigen Ausschuss des Landtages in geheimer Sitzung zu begründen. Die Entscheidung des Ausschusses kann veröffentlicht werden (§§ 11 Abs. 2 Satz 2 AIG, 26 Abs. 2 BbgDSG).

2 Umsetzung des Brandenburgischen Akteneinsichts- und Informationszugangsgesetzes

2.1 Die Nutzung des Akteneinsichtsrechts - keine Statistik, kein Überblick

Wieviele Anträge auf Akteneinsicht wurden 1999 gestellt? Bei welchen Behörden gingen die häufigsten Anträge ein? Welche Themen interessierten die Antragstellerinnen und Antragsteller am meisten?

Solche und ähnliche Fragen kommen fast täglich. Fragen, deren Antworten einen interessanten Aufschluss über die Nutzung des neuen Rechts in Brandenburg geben könnten.

Im vergangenen Jahr teilte der Minister des Innern im Rahmen der Beantwortung einer Kleinen Anfrage zur Ausgestaltung des Akteneinsichtsrechts im Namen der Landesregierung mit, dass bis zum Stichtag 30.06.1998 auf der Grundlage des Brandenburgischen Akteneinsichts- und Informationszugangsgesetzes (AIG) 27 Anträge gestellt

wurden[74]. Die Zählung schloss allerdings lediglich die Landesministerien und deren nachgeordnete Behörden und Einrichtungen ein und bezog sich gerade einmal auf einen Zeitraum von vier Monaten nach In-Kraft-Treten des Gesetzes. Im Februar 1999 teilte der Minister auf eine ähnlich lautende Anfrage mit, es seien im gesamten Jahr 1998 68 Anträge nach AIG gestellt worden[75]. Gleichzeitig schränkte er die Aussagefähigkeit dieser Angabe durch den Hinweis darauf ein, dass die Akten führenden Behörden Anträge nach dem AIG in der Regel ohne Beteiligung der jeweiligen Aufsichtsbehörde bescheiden. Ungenauigkeiten seien deshalb nicht auszuschließen. In einer weiteren Anfrage zu den Fällen im 1. Halbjahr 1999 gibt der Minister des Innern die Zahl der in den Landesministerien gestellten Anträge mit 14, die im nachgeordneten Bereich mit 11 an[76]. Allerdings hätten nicht alle Ressorts Angaben zu den Einsichtsbegehren in den nachgeordneten Bereichen gemacht.

Die Schwierigkeiten des Innenministeriums, hier eine genaue Auskunft zu geben, liegen darin begründet, dass eine systematische, alle Verwaltungsebenen umfassende Statistik bisher nicht erstellt wird. Während es für die obersten Landesbehörden noch relativ unkompliziert ist, die dort gestellten Anträge zu erfassen, ist diese Aufgabe für den nachgeordneten Bereich ohne einheitliche Vorgaben schon nicht mehr zu bewerkstelligen. Die kommunalen Verwaltungen waren von vornherein nicht Gegenstand der Antwort der Landesregierung.

Dabei sind die obersten Landesbehörden in den wenigsten Fällen erste Ansprechpartnerinnen für die Akteneinsicht der Bürgerinnen und Bürger. Der direkte Kontakt zur Verwaltung findet in einem Flächenland wie Brandenburg zumeist vor Ort statt, also in den Gemeinden, Ämtern, Städten und Kreisen. Es ist deshalb davon auszugehen, dass hier auch die Nachfrage nach Informationen der Verwaltungen am Größten ausfallen dürfte. Auch wenn einige Kommunen - als positives Beispiel sei hier die Landeshauptstadt Potsdam erwähnt - bereits aus eigener Initiative eine Statistik zu den dort gestellten Anträgen auf Akteneinsicht führen, bleibt dies doch so lange Stückwerk, bis erstens alle Verwaltungen, die dem AIG unterliegen, dies in gleicher Weise handhaben und zweitens diese Statistiken zentral zusammengeführt werden.

---

74 LT-Drs. 2/6098

75 LT-Drs. 2/6098

76 LT-Drs. 2/6575

Staaten, die schon länger über Informationszugangsgesetze verfügen, haben darin die Verpflichtung zum Führen einer Statistik festgeschrieben. In den USA ließ sich so der Anstieg der Nachfrage nach Verwaltungsinformationen kontinuierlich verfolgen. Faktoren konnten analysiert werden, die den Umgang mit der Informationsfreiheit nachhaltig veränderten. So berichtete der ehemalige Chief Counsel des Sub-Committee on Government Information des US-Senats, Dr. Gellman, über eine deutliche Abnahme der Zahl der Anträge, seit bestimmte Behörden freiwillig Informationen ins Internet einstellen[77]. Auch gibt eine solche Übersicht Hinweise darüber, in welchen Aufgabengebieten der Verwaltung der Informationsbedarf der Bürgerinnen und Bürger am Größten ist bzw., ob die Bearbeitung der Anträge - beispielsweise in zeitlicher Hinsicht - in zufrieden stellender Form erfolgt. Eine Optimierung der Form der Informationsbereitstellung (z. B. Digitalisierung von Vorgängen) als Folge einer Auswertung erleichtert die Arbeit der Verwaltung langfristig. Auch Rückschlüsse für die Steuerung der Verwaltungsabläufe im Sinne einer erhöhten Transparenz von Entscheidungen und mehr Bürgernähe können gezogen werden. Eine jährliche Statistik ließe sich mit geringem Verwaltungsaufwand erstellen. Sie sollte folgende Angaben beinhalten:

- Akten führende Stelle, bei der der Antrag gestellt wird
- Gegenstand des Antrags (z. B. "Einsicht in Bauakten")
- Dauer der Bearbeitung
- Entscheidung über den Antrag (Einsicht gewährt / teilweise gewährt / nicht gewährt)
- Festgesetzte Gebühren
- Etwaige Widerspruchs- oder Gerichtsverfahren

Auf die Speicherung von Daten, die auf die Antrag stellende Person bezogen sind, sollte im Zusammenhang mit der Statistikerstellung verzichtet werden. Eine Zusammenführung der Statistik beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht bietet sich an.

Im Vergleich zu Staaten wie Kanada, wo in der bevölkerungsreichsten Provinz Ontario allein 1998 fast 20.000 Anträge auf Informationszugang gestellt wurden, erscheinen die vorhandenen (unvollständigen) Zahlen aus Brandenburg verschwindend gering. Selbst beim Rat der Europäischen Union wurde 1998 in 338 und allein im 1. Quartal 1999 in 385 Fällen Zugang zu Dokumenten beantragt. Daraufhin wurden jeweils 82,4 bzw. 91,8% aller Dokumente freigegeben. Aber die Zahlen aus Brandenburg erscheinen in einem anderen Licht, wenn man bedenkt, dass hier ein Gesetz anzuwenden ist, das mit einer langen Rechtstradition der Geheimhaltung bricht.

---

[77] Vortrag beim Internationalen Symposium "Informationsfreiheit und Datenschutz" am 25./26.10.1999 in Potsdam

Eine statistische Erfassung der Anträge auf Akteneinsicht sollte in allen brandenburgischen, dem AIG unterliegenden Verwaltungen erfolgen und könnte in Form jährlicher Berichte beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zusammengeführt werden.

2.2 Neuland für die Verwaltung - Wie reagieren die Behörden?

Wie stellt die Verwaltung sicher, dass die Umsetzung des Rechts auf Akteneinsicht in allen Behörden nach einheitlichen Grundsätzen erfolgt?

Das Ministerium des Innern veröffentlichte im September 1998 "Erste Hinweise zur Anwendung des AIG"[78]. Dieses Arbeitspapier dient den Verwaltungen als wichtige Hilfestellung bei der Auslegung des komplizierten Gesetzestextes. In Beantwortung einer Kleinen Anfrage teilte der Minister des Innern im Namen der Landesregierung im Oktober 1998 mit, dass wegen der ressortspezifischen Besonderheiten in den Ministerien unterschiedliche Verfahrensordnungen bestehen bzw. in Vorbereitung waren[79]. Wir haben deshalb in einigen Ministerien nachgefragt und um Zusendung der jeweiligen internen Verwaltungsanweisungen gebeten.

Während einige Ministerien in ihren Antworten teilweise auf das vom Innenministerium erstellte Arbeitspapier Bezug nahmen, haben andere eigene Hinweise erarbeitet:

Danach verpflichtet das Ministerium der Finanzen seinen nachgeordneten Bereich Anträge dem Fachreferat des Ministeriums auf dem Dienstweg vorzulegen, der Antragstellerin bzw. dem Antragsteller eine Zwischennachricht zu senden, das Rechtsreferat an der Entscheidung zu beteiligen und den Abteilungsleitungen das Ergebnis der Prüfung vor Abgang zur Kenntnis vorzulegen. Diese Vorgehensweise stellt einerseits die einheitliche Bearbeitung der Anträge sicher und trägt somit dem Grundsatz der Gleichbehandlung Rechnung. Andererseits bedeutet die Beteiligung der obersten Landesbehörde für nachgeordnete Behörden oder Einrichtungen eine zeitliche Verzögerung, die im Hinblick auf die beim Informationszugang entscheidende Aktualität der begehrten Informationen kritisch zu beurteilen ist. Unseres Erachtens würde eine Hilfestellung bei der Auslegung des AIG in Form einer Verfügung für den nachgeordneten Bereich ausreichen, um eine einheitliche Bearbeitung zu gewährleisten und zeitkritischen Anträgen auf Akteneinsicht dennoch zu genügen.

---

78 s. dazu Tätigkeitsbericht 1998, Pkt. B 1.3.1

79 LT-Drs. 2/5740

Das Justizministerium wiederum - soweit es Akten führende Stelle ist - beteiligt das Presse- sowie ein Rechtsreferat bei der Antragsbearbeitung. Dieses Ministerium stellt den nachgeordneten Behörden eigene Hinweise zur Verfügung, überlässt ihnen jedoch die Detailregelung. Eine solche Lösung ist aus unserer Sicht angemessen.

Eine ebenfalls zweckmäßige Bearbeitungsweise wurde im Ministerium für Ernährung, Landwirtschaft und Forsten gefunden. Der behördliche Datenschutzbeauftragte und Ansprechpartner für den Informationszugang veröffentlichte einen schematischen Bearbeitungsablauf für Anträge nach dem AIG in den Dienstnachrichten. Der Ablauf schreibt der AIG-Ansprechperson eine koordinierende Rolle bei der Bearbeitung der Anträge in der jeweiligen Behörde zu. Die eigentliche Prüfung der Anträge erfolgt jedoch - unter Berücksichtigung der Hinweise des Ministeriums des Innern - in den Fachreferaten. Nicht zuletzt durch die Einbindung der Ansprechperson für den Informationszugang und die dadurch erleichterte Terminkoordination kann eine einheitliche und zeitnahe Bearbeitung der Einsichtsanträge gewährleistet werden.

Gleichzeitig hat uns interessiert, wie in den Kommunen mit der Umsetzung des Rechts auf Akteneinsicht verfahren wird. Hierzu haben wir in vier kreisfreien Städten nach Verwaltungsanweisungen zum AIG gefragt. Während in einem Fall lediglich die Zuständigkeiten für die Bearbeitung festgelegt und in einem weiteren Fall durch eine Rundverfügung der Geschäftsgang geregelt wurden, hat die Stadt Potsdam eine ausführliche Dienstanweisung als Teil des städtischen Verwaltungshandbuchs erstellt, die sehr hilfreich ist.

Verwaltungsinterne Richtlinien zur Anwendung des AIG können die Bearbeitung der Anträge auf Akteneinsicht erleichtern und dadurch beschleunigen. Hierbei empfiehlt sich die Einbindung der Ansprechpersonen für den Informationszugang in den jeweiligen Behörden. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht berät Verwaltungen gerne bei der Erstellung solcher Vorschriften.

2.3 Gebühren und Auslagen - Was soll das Grundrecht auf Information kosten?

Noch ist unklar, welche Gebühren die Bürgerinnen und Bürger für Amtshandlungen nach dem AIG bezahlen müssen. Während die Landesgebührenordnung noch nicht beschlossen ist, erheben die Kommunen Gebühren nach eigenen Satzungen.

Das AIG ermächtigt die Landesregierung zum Erlass einer Gebührenordnung für die Akteneinsicht (§ 10 Abs. 2 AIG). Gleichzeitig bestimmt das Gesetz, dass für Amtshandlungen in Angelegenheiten der Selbstverwaltung von Gemeinden und Gemeindeverbänden die Vorschriften des Kommunalabgabengesetzes unberührt bleiben (§ 10 Abs.

3 AIG). Aus dieser Unterscheidung ergibt sich, dass für eine kommunale Verwaltung zwei unterschiedliche Maßstäbe für die Gebührenfestsetzung bei der Akteneinsicht ausschlaggebend sind: Die Landesgebührenordnung, wenn es um Akten geht, die Informationen über Auftragsangelegenheiten bzw. Pflichtaufgaben zur Erfüllung nach Weisung enthalten sowie das Kommunalabgabengesetz bzw. kommunale Gebührensatzungen für Akten, die zu Selbstverwaltungsangelegenheiten geführt werden.

Beim Akteneinsichtsrecht handelt es sich um ein in der Landesverfassung verbürgtes Grundrecht. Niemand darf durch unangemessen hohe Gebühren von dessen Wahrnehmung abgehalten werden (vgl. § 10 Abs. 1 AIG). Das AIG bestimmt, dass die Gebühren so zu bemessen sind, "dass zwischen dem Verwaltungsaufwand einerseits und dem Recht auf Akteneinsicht andererseits ein angemessenes Verhältnis besteht". In der Praxis dürfte genau dies jedoch nicht der Fall sein, wenn die Gebühren auf der Grundlage allgemeiner Verwaltungsgebührensatzungen erhoben werden. Dies liegt daran, dass sich dort die Höhe der Gebühren in der Regel nach dem Zeitaufwand bei der Bearbeitung des Antrags richtet und somit grundsätzlich nach oben hin offen ist.

Dass "Kostenregelungen in anderen Rechtsvorschriften" unberührt bleiben (§ 10 Abs. 1 AIG) kann jedoch nicht bedeuten, dass Gebührenerhebungen, wie sie z. B. gemäß Kommunalabgabengesetz bzw. den auf dessen Grundlage erlassenen kommunalen Gebührensatzungen getroffen werden, die Angemessenheit der Höhe der Gebühren außer Acht lassen dürfen.

Der Zeitaufwand als Berechnungsgrundlage ist auch schon deshalb nicht hinnehmbar, weil dadurch die Kosten für eine zurückhaltende Informationspolitik der Behörde oder sogar für etwaige organisatorische Mängel (z. B. bei der Registratur oder Aktenführung) auf die Antragstellenden umgelegt werden.

Erfahrungen in den USA, wo mehr und mehr Verwaltungen dazu übergehen, Informationen von sich aus ins Internet einzustellen, zeigen nicht nur, dass die Zahl der Anträge zurückgeht, sondern auch, dass dadurch Kosten gesenkt werden können: Während die Bearbeitung der Anträge in jedem Einzelfall zeitaufwendig sein kann, ist die freiwillige Veröffentlichung von Informationen insbesondere im Hinblick auf die Möglichkeiten des Internets wesentlich kostengünstiger. Die Entscheidung, welche Kosten anfallen, liegt also auf der Seite der Verwaltung. Eine Entscheidung für höhere Kosten darf daher nicht zu Lasten der Antragstellerinnen und Antragsteller gehen.

Aus Sicht der Kommunen ist es verständlich, dass sie die Antragstellerinnen und Antragsteller nicht mit der komplizierten Unterscheidung von Gebührenarten konfrontieren möchten und für eine Übergangszeit bis zum Erlass einer Landesgebührenordnung eigene Satzungen für alle Aufgabenarten heranziehen. Es ist jedoch notwendig, zu einem einheitlichen Gebührenmaßstab zu gelangen, der auf beide Aufgabenarten angewandt werden kann und dem Gesichtspunkt der Angemessenheit der Höhe der Gebühren Rechnung trägt. Die Kommunen könnten sich

beim Erlass eigener Gebührensatzungen für das AIG nach der Landesgebührenordnung richten, um eine einheitliche Grundlage zu gewährleisten. Allerdings steht diese Rechtsverordnung noch aus. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dieses Problem gegenüber den zuständigen Ministerien zum Ausdruck gebracht.

Hinsichtlich der Gebührenordnung ist auf ein Urteil des Europäischen Gerichtshofs vom 9. September 1999 zur Vereinbarkeit des bundesdeutschen Umweltinformationsgesetzes (UIG) mit dem Gemeinschaftsrecht (der Umweltinformationsrichtlinie der EG) hinzuweisen[80]. Während die deutsche Regelung selbst im Fall der Ablehnung eine Gebühr vorsieht, ermächtigt die Richtlinie dazu lediglich für die Übermittlung von entsprechenden Informationen. Der Gerichtshof hält daher die Bestimmung des UIG für nicht mit der Richtlinie vereinbar. Der Grundsatz der Gebührenfreiheit für abgelehnte Informationsersuchen sollte auch bei der Erstellung der Landesgebührenordnung zum AIG berücksichtigt werden. Letztlich sollte der Gesetzgeber überlegen, ob nicht gänzlich auf die Gebühr zu verzichten ist und die Kosten für die Akteneinsicht als allgemeine Kosten der Verwaltung anzusehen sind, um den dahinter stehenden Prinzipien der Bürgerbeteiligung und Verwaltungstransparenz zu genügen.

Eine Landesgebührenordnung für Amtshandlungen nach dem AIG sollte schnellstmöglich erlassen werden, um eine landesweit einheitliche Gebührenerhebung zu gewährleisten. Sie hat sich am Grundsatz zu orientieren, dass die Gebühr so bemessen sein soll, dass Bürgerinnen und Bürger nicht von vornherein von der Antragstellung "abgeschreckt" werden. Für die Ablehnung der Akteneinsicht sollte keine Gebühr erhoben werden.

2.4 So anonym wie möglich - personenbezogene Daten sparsam verwenden

Ein Antrag auf Akteneinsicht ist schriftlich zu stellen. Wie gehen die Verwaltungen mit den darin enthaltenen personenbezogenen Angaben um?

Einige Verwaltungen führen bereits eine Statistik zu den Anträgen auf Akteneinsicht, die bei ihnen gestellt wurden. Dies ist zu begrüßen. In einer Kommune wird hierzu ein "Kontrollblatt" erstellt, das in halbjährlichen Abständen als Grundlage für eine Berichterstattung an die Stadtverordnetenversammlung dient. Das Kontrollblatt gibt Auskunft über das Datum der Antragstellung, die Akte, in die Einsicht begehrt wurde, das Ergebnis (Zustimmung/Ablehnung), das Datum des Bescheids sowie über Zeitaufwand und die erhobene Gebühr. Allerdings wird im Kontrollblatt auch der Name der Antragstellerin bzw. des Antragstellers verzeichnet. Obwohl es keinen Anlass gibt, dies zu

[80] s. oben A 10.1 und B 1.2

unterstellen, besteht hierdurch grundsätzlich die Gefahr einer "Querulantendatei". Dies ist in jedem Fall zu vermeiden. Auf eine Übersicht darüber, wer wann welche Akte eingesehen hat, kann verzichtet werden, ohne dass dadurch die Aussagekraft einer Statistik an Wert verliert.

Dass Anträge auf Akteneinsicht personenbezogen bearbeitet werden müssen, ist unvermeidbar, zumal sie der Schriftform bedürfen. Ist jedoch Akteneinsicht in vollem Umfang gewährt worden und die Gebühr eingegangen, müssen die personenbezogenen Daten gelöscht werden. Eine weitere Speicherung ist unzulässig.

Daten mit Bezug zu den Antrag stellenden Personen dürfen nur zur Vorgangsbearbeitung verwendet werden. In einer statistischen Übersicht zur Nutzung des AIG sind sie unzulässig.

3 Erfahrungen mit Anträgen auf Akteneinsicht

3.1 Eingaben und Anfragen beim Landesbeauftragten - Information und Unterstützung bei Problemen

Wo kann ich erfahren, ob es in meinem Fall sinnvoll ist, einen Antrag auf Akteneinsicht zu stellen? An wen kann ich mich wenden, wenn mein Antrag abgelehnt wurde?

Seit der Verabschiedung des Gesetzes im Jahre 1998 rückt die neue Aufgabe des Landesbeauftragen für den Datenschutz und für das Recht auf Akteneinsicht zunehmend ins Bewusstsein von Verwaltung und Öffentlichkeit. Der Landesbeauftragte ist immer häufiger der erste Ansprechpartner, wenn es um Fragen der Akteneinsicht geht. Bürgerinnen und Bürger wenden sich an uns, wenn sie wissen möchten, was das AIG für sie überhaupt bedeutet und wie sie es nutzen können. Verweigern Behörden ihnen die Einsicht, beschweren sie sich bei uns darüber. Wir bemühen uns um Aufklärung des Sachverhalts und setzen uns für die Wahrung des Grundrechts auf Akteneinsicht und Informationszugang ein. Häufig sind aber auch Verwaltungen unsicher, wie das AIG auf einen ganz speziellen Fall anzuwenden ist und bitten uns um Unterstützung, die wir gerne bieten.

Wie nicht anders zu erwarten, wird der größte Teil der Anträge von einzelnen Privatpersonen gestellt. Einen großen Anteil nahmen Anfragen von Verwaltungen ein, die sich zumeist zur Bearbeitung von Anträgen bei uns beraten ließen. Der Anteil von Mandatsträgerinnen und -trägern (Landtagsabgeordnete, kommunale Vertretungen) ist gering, was auch dadurch zu erklären ist, dass dieser Personenkreis sehr viel weitergehende, teilweise in der Verfassung verankerte Auskunfts- und Informationsrechte hat. Auch ist die Presse im Berichtsjahr nur selten an uns

herangetreten, im Gegensatz zu den USA, wo das dortige Informationsfreiheitsgesetz zu einem großen Teil von ihr genutzt wird.

Dass die Presse bisher nicht sehr häufig Einsichtsrechte nach dem AIG geltend gemacht hat, mag damit zusammenhängen, dass das Verfahren bis zur Entscheidung über den Informationszugang zu schwerfällig und für schnelle Recherchen zu zeitaufwendig ist. Häufig führt der presserechtliche Auskunftsanspruch schneller zum Ziel. Aber für einen Hintergrundbericht oder eine längerfristige Recherche kann durchaus sinnvoll sein, vom Recht auf Einsicht in Originalunterlagen Gebrauch zu machen, das den Journalistinnen und Journalisten neben dem presserechtlichen Auskunftsanspruch zusteht (allerdings im Gegensatz zu diesem gebührenpflichtig ist)[81].

3.2 Spezialgesetze und das AIG - worauf stütze ich meinen Einsichtsantrag?

Wer sich an uns wendet, fragt zumeist nach einer Akteneinsicht auf der Grundlage des AIG. Aber es kommen auch andere Rechtsgrundlagen in Frage.

[81] s. Tätigkeitsbericht 1998, Pkt. B 4.2

Soweit es um Daten geht, die sich auf die Antrag stellende Person selbst beziehen, ergibt sich ein Akteneinsichtsrecht schon aus dem Brandenburgischen Datenschutzgesetz (§ 18 Abs. 4), das dem Betroffenen eine sehr viel stärkere Rechtsstellung einräumt als das Akteneinsichtsgesetz[82]. Aber auch in anderen Fällen wird dieses allgemeine Informationszugangsgesetz häufig von anderen speziellen Vorschriften verdrängt, die ebenfalls Akteneinsicht ermöglichen. So können Personen, die an einem laufenden Verwaltungsverfahren beteiligt sind, dort ohnehin Einsichtsrechte auf der Grundlage des Verwaltungsverfahrensgesetzes geltend machen. Dies ist den Bürgerinnen und Bürgern meist nicht bekannt. Nach Prüfung der Anliegen, die an uns herangetragen wurden, stellte sich heraus, dass für fast ein Drittel der Fälle die Anspruchsgrundlage für Akteneinsicht in speziellen Gesetzen zu finden ist.

Offenbar wenig bekannt, aber in der Praxis bedeutsam ist das Umweltinformationsgesetz (UIG). Es gewährt Interessierten den Zugang zu allen bei Behörden vorhandenen Informationen über die Umwelt. Beispielsweise wandte sich eine Stadtverwaltung mit der Bitte an uns, sie bei der Entscheidung eines Einsichtsantrags nach AIG zu unterstützen. Ein Bürger fühlte sich durch Lärm und Geruch belästigt, begehrte Einsicht in Akten über einen Landwirtschaftsbetrieb und berief sich auf das AIG. Hier handelt es sich jedoch um Umweltinformationen, sodass der Antrag nicht auf der Grundlage des AIG, sondern des UIG zu prüfen ist.

Der Vorrang von Spezialgesetzen mag auf den ersten Blick unübersichtlich sein. Häufig bieten diese jedoch einen weitergehenden Einsichtsanspruch, als dies nach dem AIG möglich wäre. Insbesondere besteht in speziellen Regelungen häufig die Pflicht der Behörde zur Abwägung der vorgebrachten Interessen, während das AIG für einige Ausnahmetatbestände recht strikte Maßgaben zur Verweigerung der Akteneinsicht beinhaltet. Das gilt auch für den Anspruch auf Akteneinsicht nach allgemein rechtsstaatlichen Grundätzen oder nach dem Grundsatz von Treu und Glauben. Dieser setzt zwar ein berechtigtes Interesse an der begehrten Information voraus, bei dessen Vorliegen kann aber ein Einsichtsanspruch sogar dann bestehen, wenn nach dem Akteneinsichtsgesetz der Informationszugang aufgrund einer Ausnahme versagt werden müsste[83].

Angesichts dieser komplizierten Rechtslage kann von den Bürgerinnen und Bürgern nicht erwartet werden, dass sie ihr Anliegen auf die richtige Rechtsgrundlage stützen. Wendet sich ein Beschwerdeführer an uns unter Berufung auf das AIG, das möglicherweise in seinem Fall nicht weiterhilft, so halten wir es für unsere Pflicht, ihn umfassend über seine rechtlichen Möglichkeiten auch nach anderen Vorschriften (z. B. Verwaltungsverfahrensgesetz, Pressegesetz) aufzuklären. Formelle Befugnisse zur Beanstandung stehen dem Landesbeauftragten allerdings nur bei festgestellten Verstößen gegen das Akteneinsichts- und Informationszugangsgesetz zu (§ 11 Abs. 2 Satz 2 AIG).

---

82 s. Tätigkeitsbericht 1998, Pkt. B 2.1

83 So das VG Potsdam LKV 1999, S. 155 f.

Nicht immer ist das AIG die richtige Grundlage für eine Akteneinsicht. Informationen über die Umwelt können mit Hilfe des Umweltinformationsgesetzes eingesehen werden. Verfahrensbeteiligte haben spezielle Einsichtsrechte, insbesondere auf der Grundlage des Verwaltungsverfahrensgesetzes. Spezielle Gesetze und das Rechtsstaatsprinzip können im Einzelfall einen weitergehenden Informationszugang ermöglichen als das AIG.

3.3 Eingaben beim Landesbeauftragten - die Erfolgsaussichten

In der Hälfte der Fälle, deren Ergebnis uns bekannt ist und in denen wir eine fallbezogene, d. h. nicht auf eine allgemeine Beratung beschränkte Unterstützung leisteten, wurde die Einsicht gewährt, nachdem die Antragstellenden sich an uns gewandt haben.

Teilweise mussten wir feststellen, dass die Ablehnung eines Antrags den Regelungen des AIG entspricht. In der Regel ging es dabei um die Schutzbedürftigkeit personen- oder unternehmensbezogener Daten. Allerdings kam es auch vor, dass Anträge an Institutionen gerichtet wurden, die dem AIG gar nicht unterliegen. Eine Antragstellerin begehrte Einsicht in die Unterlagen einer kommunalen Wohnungsbaugesellschaft. Dies wurde von der Gesellschaft zu Recht abgelehnt, da für sie als privatrechtliche GmbH das AIG nicht gilt. Hier konnten wir jedoch zumindest insofern weiterhelfen, als wir empfahlen, einen Antrag auf Einsicht in die bei der Kommune vorhandenen Unterlagen zu stellen.

In den meisten Fällen führte die Anrufung des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zum Erfolg. In einigen Fällen war die Ablehnung des Antrags jedoch rechtmäßig.

3.4 Schwerpunkte der Eingaben und Anfragen

Einsicht kann in die Akten aller brandenburgischen Behörden genommen werden. Wir gehen aber davon aus, dass Anträge vor allem bei jenen Verwaltungen gestellt werden, mit denen die Bürgerinnen und Bürger direkten Kontakt haben, also bei den Kommunen. Ministerien dürften unserer Einschätzung nach nicht so häufige Adressaten von Einsichtsanträgen sein[84].

Vorrangig betrafen die bei uns gemachten Eingaben jedoch die Bereiche Finanzen, Inneres sowie Städtebau, Wohnen und Verkehr. Im Bereich der Finanzen ging es vor allem um die Einsichtnahme in Akten aus Restitutionsverfahren

[84] Zu den Einsichtsanträgen bei der Landesregierung s. oben Pkt. B 2.1

bzw. Liegenschaftsakten sowie andere vermögensrechtliche Unterlagen. Hierbei spielten die Einsichtsrechte von Verfahrensbeteiligten und damit spezialgesetzliche Regelungen jedoch meist eine größere Rolle als das Akteneinsichtsgesetz. Die Betroffenheit des Bereichs Inneres resultiert zum großen Teil aus Informationsbegehren hinsichtlich kommunaler Aufgaben. Hier ist zum Beispiel die Ordnungsverwaltung zu nennen.

Nahezu ein Drittel der Eingaben und Anfragen betraf den Aufgabenbereich Städtebau, Wohnen und Verkehr. Grund hierfür sind zahlreiche Fragen und Probleme, die aus dem Zuständigkeitsbereich der Bauverwaltungen an uns herangetragen wurden. Häufig begehrten Bürgerinnen und Bürger, aber auch Bürgerinitiativen Einsicht in Bauakten (z. B. in Baugenehmigungen), weil sie von bestimmten Bau- und Planungsmaßnahmen betroffen, jedoch nicht Beteiligte bzw. Nachbarn im bau- und verfahrensrechtlichen Sinne waren.
So informierte sich ein Bürger bei uns über seine Rechte, weil er wissen wollte, welche Maßnahmen zur Erschließung eines Bauprojektes vorgesehen sind bzw. welche Vorkehrungen zum Schutz des Wohngebietes (Auflagen) in der Baugenehmigung vorhanden sind. Die Verwaltung steht hier vor dem Problem, dass eine Akte sowohl die unkritischen Informationen (z. B. über die Auflagen zum Schutz des Wohngebietes), als aber auch personen- und unternehmensbezogene Daten beinhaltet. Um die Schutzrechte Dritter ausreichend zu berücksichtigen, sieht das AIG (§ 6 Abs. 2) auch eine Möglichkeit einer Teileinsicht vor. Hierzu hat die Behörde schutzwürdige Informationen beispielsweise durch Schwärzung auszusondern und die restlichen Aktenteile offen zu legen. Ist dies nicht mit verhältnismäßigem Aufwand möglich, so hat sie zumindest Auskunft zu erteilen. Es gibt bei der Akteneinsicht keine "Alles-oder-Nichts"-Regel, nach der eine Akte entweder vollständig oder überhaupt nicht offen zu legen ist.

Unsicherheiten bei der Anwendung des Gesetzes und die Neigung, die Entscheidung über die Gewährung von Akteneinsicht auf andere Behörden zu verlegen, zeigte auch der Fall einer Mutter, die Einsicht in das Protokoll eines Brandschutz- und Sicherheitsbeauftragten von der Begehung einer Grundschule nehmen wollte: die Einschulung ihres Kindes in dieser Schule stand bevor. Der Direktor des Amtes, das die entsprechende Akte führte, verwies sie zunächst an den Bürgermeister der Gemeinde, die Trägerin der Schule war, dann schlug er vor, sie solle gemeinsam mit diesem das Protokoll einsehen. Erst nach unserer Intervention wurde ihr die Einsichtnahme ermöglicht.

3.5 Aufsicht - die letzte Bastion des Amtsgeheimnisses?

Ein Bürger beantragte Akteneinsicht, um zu erfahren, welche Unterlagen die Kreisverwaltung dem Ministerium des Innern als oberster Kommunalaufsichtsbehörde zur Bearbeitung seiner Beschwerde vorgelegt hat. Er glaubte in den Akten Belege dafür finden zu können, dass ihm durch eine Änderung des Flächennutzungsplans ein existenzgefährdender wirtschaftlicher Schaden entstanden sei, dessen Ersatz er

verlangt. Das Ministerium lehnte den Antrag mit der Begründung ab, dass Aufsichtsakten nicht eingesehen werden dürften.

Nachdem der Petent bei einem vorangegangenen Rechtsstreit über die Einsicht in andere Verwaltungsunterlagen erst nach zwei Jahren vom Oberverwaltungsgericht bescheinigt bekam, dass über seine Klage bisher vor dem unzuständigen Gericht verhandelt worden sei, wandte er sich in diesem Konflikt mit dem Innenministerium zunächst an uns, um schneller zu seinem Recht zu kommen. Das Ministerium legte ihm nahe, zunächst die Einsicht beim Landkreis zu beantragen, was er tat. Der Landkreis wiederum leitete den Einsichtsantrag an das Ministerium weiter, weil dieses Akten führende Stelle in dieser Angelegenheit sei.

Wir haben die fraglichen Unterlagen beim Ministerium des Innern eingesehen, um uns selbst ein vollständiges Bild von der Angelegenheit machen zu können. Die Akte enthält keine Unterlagen, die aufgrund ihres Inhalts dem Bürger vorenthalten werden müssen. Sie enthält vielmehr Unterlagen, die geeignet sein könnten, den Bürger davon zu überzeugen, dass eine weitere Verfolgung seiner Schadensersatzforderung wenig aussichtsreich ist. Das Ministerium beruft sich jedoch auf eine Ausnahmebestimmung im Akteneinsichtsgesetz, nach der Unterlagen, die der Aufsicht über eine andere Stelle dienen, von der Einsicht ausgeschlossen sind (§ 4 Abs. 1 Nr. 5 AIG).

Diese Regelung rechtfertigt es jedoch nicht, dem Bürger die gesamte Akte vorzuenthalten. Vielmehr ist auch hier durch die teilweise Gewährung von Einsicht und Aussonderung evtl. schutzwürdiger Informationen dem Informationsinteresse des Bürgers Rechnung zu tragen. Hinzu kommt, dass der Petent sich sogar als Betroffener auf das Datenschutzgesetz berufen kann, weil die streitige Akte Informationen zu seiner Beschwerde und damit zu seiner Person enthält. Das Datenschutzgesetz schränkt den Anspruch auf Akteneinsicht aber nicht in vergleichbarer Weise ein wie das Akteneinsichtsgesetz. Schließlich hat der Petent auch ein berechtigtes Interesse an der Information, weil er sie zur Durchsetzung vermeintlich bestehender Rechtsansprüche benötigt.

Zudem ist der Unmut des Bürgers nur zu gut zu verstehen, wenn er "von Pontius zu Pilatus" geschickt wird, um dann von der Kreisverwaltung mitgeteilt zu bekommen, dass das Innenministerium doch der richtige Ansprechpartner für seinen Antrag sei. Mit seiner unnachgiebigen Haltung hat das Innenministerium den Petenten zu einer erneuten Klage vor dem Verwaltungsgericht veranlasst. Dieser Rechtsstreit wäre wahrscheinlich durch rechtzeitige partielle Einsichtsgewährung zu vermeiden gewesen.

In einem anderen Fall beantragte ein Journalist Einsicht in eine fachaufsichtliche Weisung, die das Justizministerium der Staatsanwaltschaft in einem Ermittlungsverfahren gegen ein ehemaliges Mitglied der Landesregierung erteilt hatte. Das Verfahren hat inzwischen zur Verurteilung des Angeklagten geführt. Das Ministerium behandelte diesen Antrag zwar nach dem Akteneinsichts- und Informationszugangsgesetz,

lehnte aber eine Offenlegung der Weisung mit dem Hinweis auf die Ausnahmeregelung für Aufsichtsakten ab.

Der Sinn dieser Regelung besteht nach Auffassung des Ministeriums darin, dass der "interne Willensbildungs- und Abstimmungsprozess zwischen Behörden im Rahmen der Rechts- und Fachaufsicht besonders geschützt werden" soll. Zudem könnten "Aufsichtsmaßnahmen leicht als bewertende Kritik empfunden werden, deren negative Auswirkungen auf den Betroffenen durch die "Gefahr" der Kenntnisnahme durch Dritte noch intensiviert würden".

Dieser Auffassung kann sich der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht nicht anschließen. Willensbildung und Abstimmung zwischen den Behörden genießen, sofern sie abgeschlossen sind, nicht von vornherein einen höheren Schutz als andere Informationen.

Ziel der politischen Mitgestaltung ist gerade die Herstellung von Transparenz des Verwaltungshandelns - hierzu zählen auch interne Abstimmungen und Weisungen. Daher ist nicht zu erkennen, wieso Aufsichtsmaßnahmen, selbst wenn sie als Kritik verstanden werden könnten, geheim zu halten sind. Sollte eine solche Maßnahme gegenüber nachgeordneten Stellen der (Wieder-)Herstellung eines rechtmäßigen Zustandes dienen, ist deren Bekanntwerden vielmehr geeignet, das Vertrauen der Bürger in die Verwaltung zu stärken. Das Akteneinsichtsrecht als politisches Mitgestaltungs- und Kontrollrecht lebt davon, dass nicht nur die "guten Taten" der Verwaltung nach außen hin dargestellt, sondern auch Problemgebiete bekannt werden.

Nur soweit in Akten Informationen enthalten sind, die aus anderen Gründen geheimhaltungsbedürftig sind, erscheint es gerechtfertigt, diese Informationen auch nicht in solchen Akten zugänglich zu machen, die zu Zwecken der Aufsicht geführt werden.

Am Beispiel der Aufsichtsakten wird zugleich die Bedeutung des § 6 Abs. 2 AIG deutlich: Zwar enthalten die §§ 4 und 5 AIG strikte Ausnahmetatbestände zum Schutz öffentlicher und privater Belange, jedoch sind nach § 6 Abs. 2 Akten, die schutzwürdige Informationen enthalten, auf dem Wege der Aussonderung von Aktenteilen oder Einzeldaten zumindest teilweise offen zu legen.

Akten, die zur Aufsicht über eine andere Stelle dienen, sind nicht von vornherein insgesamt von der Möglichkeit einer Einsichtnahme ausgeschlossen. Durch eine Aussonderung schutzwürdiger Aktenbestandteile ist hier wie auch in anderen Fällen der übrige Teil der Akte offen zu legen.

3.6 Informationszugang und der Zeitfaktor - politische Mitgestaltung im Wartestand

Der Zugang zu Verwaltungsinformationen wird nicht ausschließlich dadurch verhindert, dass Behörden Anträge auf Akteneinsicht ablehnen. Bereits das Ausschöpfen der maximalen Bearbeitungsfrist von drei Monaten, bevor eine "Untätigkeitsklage" nach § 75 Verwaltungsgerichtsordnung (VwGO) zulässig ist, reicht aus, Informationen veralten und somit einen Antrag ins Leere laufen zu lassen.

Insbesondere bei eiligen Anliegen der Antrag stellenden Personen kann bereits eine Bearbeitungszeit von drei Wochen - die rechtlich an sich nicht zu beanstanden ist - zu Schwierigkeiten führen. So kann beispielsweise ein Journalist nicht Wochen lang auf Informationen warten, die im tagespolitischen Geschehen eine Rolle spielen und bei Antragsgewährung längst nicht mehr aktuell sind. Auch für Bürgerinnen bzw. Bürger oder Interessengruppen, die beispielsweise im Zusammenhang mit einem Bürgerbegehren termingebunden Informationen der Verwaltung benötigen, hat eine lange Bearbeitungszeit dasselbe Ergebnis wie ein ablehnender Bescheid. Sie werden durch die anhaltende Unsicherheit über das Verfahrensergebnis möglicherweise sogar noch stärker beeinträchtigt.

Der Tatsache, dass Informationen immer schneller veralten und eine mehrmonatige Bearbeitungszeit dem Anliegen von Informationszugangsrechten entgegen läuft, hat beispielsweise Kanada Rechnung getragen und eine maximale gesetzliche Bearbeitungsfrist von dreißig Tagen festgeschrieben. Eine solche Regelung könnte in Brandenburg auch ohne Gesetzesänderung angewandt werden, indem Verwaltungen eine vergleichbare Frist in ihre internen Verwaltungsanweisungen zum AIG aufnehmen und danach verfahren.

Veraltete Informationen nützen niemandem. Die Verwaltungen sollten eine Frist von 30 Tagen zwischen Antragstellung und Bescheid nicht überschreiten.

4 Technisch-organisatorische Voraussetzungen der Akteneinsicht

4.1 Aktenführung und Computerdateien - der Landesbeauftragte im Praxistest

Ein Antrag auf Akteneinsicht muss hinreichend bestimmt sein. Oftmals fällt dies jedoch schwer, weil nicht bekannt ist, welche Akten in der Behörde bearbeitet werden - von Computerdateien ganz zu schweigen.

Praktische Erfahrungen mit der Bearbeitung von Einsichtsanträgen konnte der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht im Berichtszeitraum in der eigenen Behörde sammeln. Zwar ist er - abgesehen von Verwaltungsaufgaben - nicht verpflichtet, Akteneinsichtsrecht zu gewähren (§ 2 AIG). Wir haben uns

dennoch entschlossen, einen entsprechenden Antrag nach den Grundsätzen des Akteneinsichts- und Informationszugangsgesetzes zu bearbeiten. Der Antrag beschränkte sich auf Vorgänge nach dem AIG und diente der wissenschaftlichen Untersuchung der Anwendung dieses Gesetzes. Einerseits kann und will sich der Landesbeauftragte für das Recht auf Akteneinsicht dem Transparenzgedanken, dessen Umsetzung er von anderen Verwaltungen fordert, nicht für die eigene Behörde verschließen; zudem waren wir daran interessiert, einmal die Rollen zu tauschen und als Akten führende Stelle selbst den Einsichtsantrag zu bearbeiten. Andererseits müssen sich Bürgerinnen und Bürger darauf verlassen können, dass ihre Eingaben beim Landesbeauftragten vertraulich behandelt werden.

Wir sind in diesem Fall von Folgendem ausgegangen:

- Eingaben werden Dritten nicht zur Einsicht vorgelegt. Der Antragsteller hat uns auch nicht gebeten, die Einwilligung von Petenten einzuholen. Auf die Notwendigkeit der Trennung von schutzwürdigen - insbesondere personenbezogenen - und einsichtsfähigen Daten wurde bereits im letzten Tätigkeitsbericht hingewiesen[85]. Es dient sowohl der Umsetzung des Akteneinsichtsrechts als auch der Erleichterung der Arbeit der Verwaltung, wenn schon beim Anlegen von Vorgängen auch die Voraussetzungen für die Aussonderung schutzwürdiger Daten geschaffen werden.

- Einem Vorgang können vorab Kategorien wie "einsichtsfähig", "teilweise einsichtsfähig" oder "nicht einsichtsfähig" zugewiesen werden. Dies kann zwar die Prüfung im Einzelfall nicht ersetzen, sie aber wesentlich erleichtern. Das Ergebnis der Prüfung kann in den unterschiedlichen Bearbeitungsstadien des Vorgangs auch verschieden ausfallen.

- Von niemandem kann verlangt werden, von vornherein zu wissen, welche Akten eine Behörde führt. Oftmals bereitet deshalb die Bezeichnung eines konkreten Vorgangs Schwierigkeiten. Das AIG trägt dem Rechnung, in dem es der Akten führenden Stelle die Beratung und Unterstützung bei der Bestimmung des Antrags vorschreibt. Dies wird von den Verwaltungen derzeit vermutlich zumeist im Einzelfall erledigt. Sinnvoll könnte es sein, die Aktenpläne von vornherein zu veröffentlichen[86]. Hierzu bieten sich das Internet, aber auch amtliche Veröffentlichungen oder die Auslage in den Verwaltungen an. Dem Transparenzgedanken würde Rechnung getragen, wenn Interessierte sofort erkennen könnten, welche einzelnen Themen bzw. Sachgebiete die Behörden bearbeiten. Sind Aktenpläne, die veröffentlicht werden könnten, noch gar nicht vorhanden, so sollten sie umgehend erstellt werden.

---

85 s. Pkt. B 3.1

86 s. Aktenplan des LDA, Anlage 4

- Wenn Dokumente, die nicht Bestandteil eines Schriftverkehrs sind, nur in elektronischer Form vorhanden sind, unterliegen sie ebenfalls dem Aktenbegriff des AIG (vgl. § 3 AIG). Wichtig sind daher klare Verzeichnisstrukturen, die sich am Aktenplan orientieren. Beim Umgang mit Dateien sind ähnliche organisatorische Grundsätze zu beachten wie bei Akten in Papierversion, allerdings sollte der speziellen Problematik (z. B. Archivierung oder Migration von Dateien, Umgang mit elektronischer Post etc.) durch Organisationserlasse bzw. Geschäftsordnungen in den Verwaltungen Rechnung getragen werden.

Die Veröffentlichung von Aktenplänen ist notwendig, damit Antragstellerinnen und Antragsteller von vornherein wissen, welche Sachgebiete in der Verwaltung bearbeitet werden. Die Struktur von Verzeichnissen über elektronische Dateien sollte sich am jeweiligen Aktenplan orientieren.

4.2 Internet und "elektronische Akteneinsicht"

Welche Möglichkeiten bietet das Internet, um Verwaltungsinformationen transparenter und bürgernäher zu vermitteln?

Noch bestehen die Internetseiten vieler Kommunen und Verwaltungen lediglich aus ein paar Fotografien oder Grafiken und verweisen auf postalische Adressen. Allerdings wird das Internet immer häufiger auch als Medium zur gezielten Informationsvermittlung eingesetzt. Neben den hierbei üblichen touristischen Hinweisen oder Übersichten zu den Öffnungszeiten der Verwaltungen können auch Informationen ins Netz gestellt werden, die für die Bürgerinnen und Bürger notwendige Voraussetzung für die Ausübung ihrer politischen Mitgestaltungsrechte sind.

In den USA hat in den vergangenen Jahren eine zunehmende Zahl von Behörden detailliertere Verwaltungsinformationen von sich aus ins Netz eingespeist. Bisher war man dort ein jährlich steigendes Antragsaufkommen gewohnt. Durch die freiwillige Nutzung des Internets für die Vermittlung von Informationen, die ansonsten in jedem Einzelfall hätten herausgegeben werden müssen, wird nun über eine deutliche Abnahme der Zahl der Anträge berichtet. Das Vorhandensein des Rechts auf Informationsfreiheit hat dort zu mehr Transparenz geführt, ohne dass die Offenlegungen überhaupt beantragt worden wären. Die nordamerikanischen Behörden verstehen Informationsfreiheit zu Recht als eigene Bringschuld.

Als Vorstufe zu einer weit angelegten Informationsbereitstellung einsichtsfähiger Unterlagen könnten Behörden bereits kurzfristig jene Informationen im Internet bereitstellen, die sie für ihre eigene Arbeit verwenden.

Beispielsweise sind Satzungen, Verwaltungsvorschriften und Erlasse, aber auch Protokolle öffentlicher Sitzungen kommunaler Vertretungen hierfür geeignet.

Die Internet-Technologie ist aber keine Einbahnstraße, vielmehr ist auf dieser Basis auch die Möglichkeit einer interaktiven Verwaltung gegeben. Das Akteneinsichtsrecht bietet sich an, um diese neue Möglichkeit zu nutzen.

Bisher konnte die Antragstellerin oder der Antragsteller persönlich zur Behörde kommen und dort Einsicht in die Originalakte nehmen. Alternativ konnten Vervielfältigungen gefertigt werden. In beiden Fällen findet eine Akteneinsicht jedoch auf Papierbasis statt. Dass diese auch elektronisch möglich ist, beweist ein Projekt der Stadt Rathenow [87] . Für ihr Konzept einer "Elektronischen Akteneinsicht" im Rahmen des Media@Komm-Städtewettbewerbs, der auf eine Initiative des ehemaligen Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie zurückgeht, erhielt die Kommune im Januar 1999 einen Sonderpreis. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht begleitet das Vorhaben als einer der Projektpartner.

Kernstück des Projektes zur interaktiven Verwaltung ist das virtuelle Bürgeramt. Auf der Basis einer technischen Infrastruktur mit günstigen Konditionen wird die Anschlussmöglichkeit für alle Bürgerinnen und Bürger gewährleistet. Neben der Bereitstellung ständig verfügbarer Informationen im Internet über einen öffentlich zugänglichen Server sollen Informationen, die auf Antrag nach AIG verlangt werden, der Antragstellerin oder dem Antragsteller auf elektronischem Wege übermittelt werden. Der Aktenbestand der Stadt wurde analysiert und typologisiert. Je nach Relevanz sollen bereits vorhandene Akten noch digitalisiert werden. In einem mehrstufigen Verfahren sollen zunächst einfache Verwaltungstransaktionen, später auch komplizierte Anträge online gestellt und bearbeitet werden können. Gerade die Gewährung von Einsicht in Akten mit personen- oder unternehmensbezogenen Angaben ist schon papiergebunden derartig komplex mit ihren Einwilligungserfordernissen und Abwägungsnotwendigkeiten, dass eine Erledigung dieses Vorgangs über das Netz noch einige Vorarbeiten erfordern wird.

Die Legitimation und Identifizierung der Antrag stellenden Personen soll beispielsweise durch Passwörter und durch eine elektronische Signatur gewährleistet werden. Die Funktionsfähigkeit der elektronischen Signatur und eine entsprechende Sicherheitsinfrastruktur sind damit wesentliche Voraussetzungen für den Erfolg des Projektes.

Das Projekt zur "Elektronischen Akteneinsicht" wird von uns unterstützt, weil wir der Überzeugung sind, dass die Stadt Rathenow dem Modernisierungsgedanken der Verwaltung durch eine stärkere Bürgerorientierung Rechnung

---

87 s. schon Tätigkeitsbericht 1998, Pkt. A 2.5

trägt, gleichzeitig aber auch die Notwendigkeit einer sicheren Datenübermittlung und eines legitimierten Zugriffs der Benutzerinnen und Benutzer berücksichtigt.

Hier - wie bei allen anderen Vorhaben, die mit dem Internet in Zusammenhang stehen - ist stets zu berücksichtigen, dass besonders in Brandenburg die Dichte der privaten Anschlüsse an das Internet noch vergleichsweise gering ist. Auch wenn sich dies in absehbarer Zeit ändern und ein verbessertes Angebot die Nachfrage steigern dürfte, werden die herkömmlichen Kommunikationsformen wie Post, Telefon und Telefax nicht verschwinden. Im Gegenteil sollte gerade beim Informationszugang darauf geachtet werden, dass dieser für alle gleichermaßen gilt und nicht jene ins Hintertreffen geraten, die nicht mit Hilfe neuer Technologien kommunizieren.

Die Verwaltungen sollten Informationen, die nach dem AIG ohne Weiteres eingesehen werden können, von vornherein im Internet veröffentlichen. Akteneinsicht kann darüber hinaus auch auf elektronischem Wege gewährt werden, sofern eine sichere Datenübermittlung und Empfängerauthentifizierung gewährleistet ist.

Teil C

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

Unsere Bemühungen, die Dienststelle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht nach Potsdam zu verlagern, sind auch im Berichtszeitraum vom Präsidenten des Landtages nachhaltig unterstützt worden. Ein landeseigenes Dienstgebäude, das unserem Raumbedarf entspricht, ist in Potsdam vorhanden. Der Landtag wird nun darüber zu entscheiden haben, ob die für eine Instandsetzung erforderlichen Haushaltsmittel bereitgestellt werden. Es bleibt unser Anliegen, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht als Bürgerbehörde - wie die Datenschutzbeauftragten in allen anderen Bundesländern - dort angesiedelt sein sollte, wo die Bürgerinnen und Bürger eine Landesbehörde vermuten: in der Landeshauptstadt.

Die personelle Situation in der Dienststelle hat sich im vergangenen Jahr insofern etwas entspannt, als der Landtag eine zusätzliche Stelle bewilligt hatte, die zwischenzeitlich mit einem Diplom-Verwaltungswissenschaftler besetzt werden konnte. Dieser befasst sich in erster Linie mit Fragen des Akteneinsichtsrechts und der Verwaltungsoptimierung.

Im Berichtsjahr sind außerdem der langjährige Verwaltungsleiter und Referent, Manfred Groß, sowie die Koordinatorin im Bereich Recht, Marie-Luise Franzen, ausgeschieden. Ihrem Engagement beim Aufbau der Dienststelle in den vergangenen Jahren hat der Landesbeauftragte für Datenschutz und Akteneinsicht viel zu verdanken. Der personelle Wechsel führte zu einer Veränderung und Straffung der internen Organisation der Dienststelle. Die Aufgaben des Verwaltungsleiters wurden anderweitig verteilt. Ein neuer Leiter des Bereiches Recht, der zugleich Beauftragter des Haushalts ist, und ein juristischer Referent sind neu eingestellt worden.

2 Zusammenarbeit mit dem Landtag

Auch wenn eine Erörterung des Tätigkeitsberichtes 1998 und der Stellungnahme der Landesregierung hierzu im Berichtszeitraum aufgrund der Landtagswahl aus Zeitgründen noch nicht möglich war, hat der Landesbeauftragte in Gesprächen mit Abgeordneten des neu gewählten Landtages, insbesondere mit dem Vorsitzenden des Innenausschusses, seine Vorstellungen erläutern können. Noch in der Zweiten Legislaturperiode haben wir im

Hauptausschuss des Landtages zur Neufassung des ORB-Gesetzes im Rahmen einer Anhörung sowie im Ausschuss für Wissenschaft, Forschung und Kultur zur Novellierung des Hochschulgesetzes Stellung genommen.

3 Mitarbeit bei Themen der Verwaltungsoptimierung

Die Modernisierung und Reform der öffentlichen Verwaltung ist auch in Brandenburg ein vorrangiges Anliegen, um die Behörden stärker als bisher zu Dienstleistungseinrichtungen für Bürgerinnen und Bürger zu machen. Diese Bestrebungen führen auf kommunaler Ebene immer häufiger zur Einrichtung von Bürgerbüros oder zentralen Bürgerservice-Stellen, zu denen wir schon im vergangenen Jahr[88] detaillierte Empfehlungen gegeben hatten. Im Berichtsjahr hat uns u. a. die Landeshauptstadt Potsdam an ihren Vorbereitungen zur Einrichtung eines Zentralen Bürgerservices im Frühjahr 2000 beteiligt. Sie will unsere Empfehlungen berücksichtigen.

Die Landesregierung hat zur Fortführung des Prozesses der Verwaltungsoptimierung eine Zentrale Projektgruppe bei der Staatskanzlei und einen Ausschuss für Verwaltungsoptimierung als Leitungsgremium eingerichtet. Diese sollen Empfehlungen für das weitere Verfahren erarbeiten. Im Beirat sind die Gewerkschaften und die Landesregierung vertreten. Ein Mitarbeiter unserer Behörde wird zur Arbeit der Zentralen Projektgruppe hinzugezogen, soweit Belange unseres Aufgabengebiets betroffen sind.

Neben der Steuerung der Umsetzung der von der Verwaltungsstrukturkommission (VSK) zwischen 1997 und 1999 erarbeiteten Empfehlungen haben die Projektgremien unter anderem den Auftrag, den Prozess der Verwaltungsoptimierung im Bereich der gesamten Landesverwaltung zu koordinieren.

Im Koalitionsvertrag haben beide Regierungspartner vereinbart, mit Hilfe der Verwaltungsoptimierung sowohl die Effizienz als auch die Effektivität der Verwaltung zu verbessern. Dazu werden verschiedene Methoden eingesetzt. So ist beispielsweise vorgesehen, eine zentrale Koordinierungsstelle für Personalmanagement sowie eine Stellenbörse einzurichten. Letzteres dient der Umsetzung einer Rahmenvereinbarung zum Prozess der Verwaltungsoptimierung zwischen der Landesregierung und den Gewerkschaften. Wir setzen uns dafür ein, dass die Erhebung von Personaldaten zum Aufbau einer Datenbank sowie die Arbeit der Koordinierungsstelle in datenschutzgerechter Weise erfolgt. Ähnliche Tätigkeitsfelder dürften bei der Verwaltungsmodernisierung im Bereich der Informationstechnologie (Informationssysteme, Kosten-Leistungs-Rechnung, etc.) sowie in weiteren Aufgabengebieten aktuell werden.

---

[88] s. Tätigkeitsbericht 1998, Pkt. A 12

4 Kooperation mit anderen Datenschutzbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im vergangenen Jahr unter dem Vorsitz des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, Dr. Werner Kessel, in Schwerin und Rostock getagt und eine Reihe von Entschließungen zu aktuellen Themen des Datenschutzes gefasst, die in dem Band "Dokumente zum Datenschutz 1999" veröffentlicht sind. Dieser Band kann bei uns gesondert angefordert werden. Den Vorsitz für das Jahr 2000 hat turnusmäßig der neu gewählte Niedersächsische Datenschutzbeauftragte, Burckhard Nedden, übernommen.

Unter dem Vorsitz des Brandenburgischen Landesbeauftragten hat der Arbeitskreis Medien der Datenschutzkonferenz im vergangenen Jahr zweimal in Potsdam getagt und Entschließungen zu diesem Themenkreis für die Konferenz vorbereitet.

Der Landesbeauftragte hat außerdem in der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation mitgearbeitet und dort auch einhellige Unterstützung für seinen Vorschlag eines Gemeinsamen Standpunktes zu Gebäudedatenbanken gefunden[89].

Im Berichtszeitraum fanden mehrere Koordinationsgespräche mit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich statt, bei denen die beide Behörden berührenden Problembereiche erörtert wurden. Darüber hinaus wurden auch gemeinsame Prüfungen wie z. B. bei der Stadt Cottbus durchgeführt.

Im Zuge der verstärkten Zusammenarbeit zwischen Brandenburg und Berlin liegt es auf der Hand, dass die Datenschutzbeauftragten ihre Aktivitäten ebenfalls noch stärker koordinieren. Dies ist auch im vergangenen Jahr geschehen. Die Aufgabenbereiche der beiden Landesbeauftragten haben sich zudem dadurch angenähert, dass durch das neue Berliner Informationsfreiheitsgesetz der Berliner Datenschutzbeauftragte zugleich die Aufgabe des Beauftragten für Akteneinsicht zugewiesen bekommen hat. Gerade in diesem neuen Bereich könnte Berlin von unseren Erfahrungen profitieren. Wie im Vorjahr haben wir erneut gemeinsam mit dem Berliner Beauftragten für Datenschutz und Akteineinsicht die "Dokumente zum Datenschutz" als Anlagenband zu diesem Tätigkeitsbericht herausgegeben.

Auch die Zusammenarbeit mit der Datenschutzbeauftragten des Nachbarlandes Polen, Dr. Ewa Kulesza, ist 1999 verstärkt worden. Der Landesbeauftragte für Datenschutz und Akteneinsicht hat auf ihre Einladung hin in Warschau

---

[89] s. Dokumente zum Datenschutz 1999, Teil C

über die brandenburgischen Erfahrungen mit dem Informationszugangsrecht berichtet. Die polnische Datenschutzbeauftragte war zudem mit mehreren Mitarbeiterinnen und Mitarbeitern zu einem Informationsbesuch in unserer Dienststelle in Kleinmachnow, bei dem Erfahrungen im Bereich des Datenschutzrechts ausgetauscht wurden. Für die Zukunft sind weitere gemeinsame Aktivitäten vereinbart.

Im Zeitalter des Internets lassen sich Datenschutz und Informationszugang nicht mehr nur national durchsetzen. Beide Themen standen auf der Tagesordnung der XXI. Internationalen Datenschutzkonferenz in Hong Kong, die der Landesbeauftragte für Datenschutz und Akteneinsicht als Mitglied des Programmbeirats mitgestaltet hat. Er war dort auch um einen Beitrag zum entstehenden Recht des Cyberspace und dessen Auswirkungen auf den Datenschutz und um die Leitung eines Tagungsabschnitts über Datensicherheit und Datenschutz-Audit gebeten worden. Im Frühjahr 1999 hat der Landesbeauftragte außerdem für die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) einen Bericht über Datenschutzvereinbarungen für grenzüberschreitende Datenflüsse in der Online-Umgebung erstattet.

Schließlich war der Landesbeauftragte für Datenschutz und Akteneinsicht Gast bei der Jahrestagung der kanadischen Beauftragten für Datenschutz und Informationszugang in Halifax und konnte sich auf diese Weise vor Ort die langjährigen Erfahrungen zu Nutze machen, die in Kanada auf Bundesebene und auf der Ebene der Provinzen in diesen Bereichen gesammelt worden sind. Zugleich hat der Landesbeauftragte über praktische Fragen des Informationszugangs in Brandenburg und über Probleme des Exports personenbezogener Daten aus Ländern der Europäischen Union berichtet.

5 Öffentlichkeitsarbeit

5.1 Neue Veröffentlichungen

In den vergangenen Jahren erwies sich das Datenscheckheft als die gefragteste Publikation des Landesbeauftragten. Es beinhaltet neben kurzen Erläuterungen zu den Datenschutzrechten der Bürgerinnen und Bürger zahlreiche "Schecks" in Form von Mustervordrucken. So findet man im Datenscheckheft beispielsweise einen Brief an die Meldebehörde, mit dem der Weitergabe der eigenen Daten an Parteien oder Adressbuchverlage widersprochen werden kann. Mit einem anderen Vordruck kann z. B. von der Polizei Auskunft über die zur eigenen Person gespeicherten Daten verlangt werden. Die Vordrucke können ohne weiteren Aufwand an die betreffenden Stellen geschickt werden, um dort die eigenen Rechte in Anspruch zu nehmen. Das Datenscheckheft wurde im Berichtsjahr auf Grund veränderter Rechtsgrundlagen und angesichts der Entwicklungen beispielsweise auf dem Gebiet der Medien und Telekommunikation aktualisiert und um einen Teil zum Akteneinsichtsrecht erweitert.

Wir haben außerdem damit begonnen, die wichtigsten informationsrechtlichen Regelungen in einer Gesetzessammlung "Brandenburgisches Informationsgesetzbuch" zu veröffentlichen, das nach und nach fortgeführt werden soll. Als erstes sind das neu gefasste Brandenburgische Datenschutzgesetz und das Akteneinsichts- und Informationszugangsgesetz als Broschüren herausgegeben worden, die den Grundstein dieses Informationsgesetzbuches bilden. Wir greifen eine Idee des Berliner Datenschutzbeauftragten auf, die mittlerweile auch vom Deutschen Juristentag weiter verfolgt wird[90].

Um den Einsatz der Informationstechnik für die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung geht es in unserer aktualisierten Broschüre "Technisch-organisatorische Aspekte des Datenschutzes". Diese wurde an die veränderten Bestimmungen des neuen Brandenburgischen Datenschutzgesetzes angepasst und soll Bürgerinnen und Bürger in die Lage versetzen, eine sichere Verarbeitung ihrer Daten zu gewährleisten aber auch der Verwaltung Hinweise geben, wie sie Schwachstellen bei der Datenverarbeitung erkennen und beseitigen kann. Der Informationsschrift liegt eine CD-ROM bei, die zusätzliche, interessante Materialien zu Fragen des Datenschutzes und der Datensicherheit enthält, darunter u. a. das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik.

Die Veröffentlichungen des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht können bei uns kostenlos bestellt werden und sind auch auf unseren Internet-Seiten (http://www.lda.brandenburg.de) zu finden. Von dort können auch einzelne Schecks aus unserem Datenscheckheft abgerufen werden.

5.2 Akteneinsicht und Informationszugang

Wie bereits im vergangenen Berichtsjahr bildete das Akteneinsichts- und Informationszugangsgesetz einen Schwerpunkt der Öffentlichkeitsarbeit. Bei den Anfragen und Eingaben, die uns im Verlauf des Jahres erreichten, aber auch im Gespräch mit Bürgerinnen und Bürgern stellte sich oftmals heraus, dass vielen die Möglichkeit, Einsicht in Verwaltungsunterlagen zu nehmen, noch nicht bekannt ist. Dies dürfte umso mehr für jene gelten, die den Weg zu uns gar nicht erst einschlagen. Auch bestehen seitens der Verwaltung noch Unsicherheiten, wie mit Anträgen auf Akteneinsicht umzugehen ist. Unsere Arbeit konzentrierte sich folglich sowohl auf die Darstellung des AIG in der Öffentlichkeit als auch auf die Information der Verwaltung.

---

[90] s. Tätigkeitsbericht 1998, Einleitung

Der von uns herausgegebene "Wegweiser zur Akteneinsicht", der Erläuterungen zu den Möglichkeiten der Einsichtnahme in öffentliche Akten enthält, wurde im Sommer 1999 flächendeckend und in großer Stückzahl an die Gemeinden, Ämter, Städte, kreisfreien Städte und Landkreise Brandenburgs verteilt und von diesen zum großen Teil vor Ort ausgelegt. Hintergrund dieser Aktion war die Überlegung, dass Informationen zur Akteneinsicht den Bürgerinnen und Bürgern dort angeboten werden sollen, wo sie den intensivsten Kontakt mit der Verwaltung haben - in den Kommunen. Dort dürfte gleichzeitig das Interesse am Informationszugang am Größten sein. Aufgrund dieser Aktion wandten sich viele Interessierte an uns, um sich genauer über ihre rechtlichen Möglichkeiten zu informieren. Auch Mitarbeiterinnen und Mitarbeiter der Verwaltung machen Gebrauch von diesem Wegweiser. In vielen Fällen bestellten Kommunen weitere Exemplare des Faltblattes oder vermittelten - beispielsweise über amtliche Anzeigenblätter - die darin enthaltenen Informationen selbst weiter. Die Aktion soll im kommenden Jahr auf weitere Behörden ausgedehnt werden. Auf Anfrage sind die Faltblätter beim Landesbeauftragten jederzeit kostenlos erhältlich.

5.3 Internationales Symposium "Informationsfreiheit und Datenschutz"

Sowohl der Informationszugang als auch der Datenschutz standen im Mittelpunkt eines Internationalen Symposiums "Datenschutz und Informationsfreiheit", das der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht im Oktober 1999 in Potsdam veranstaltet hat.

Bei der ersten bundesweiten Veranstaltung dieser Art berichteten Expertinnen und Experten aus dem In- und Ausland über ihre Erfahrungen mit den unterschiedlichen Regelungen zum Informationszugang und über das Spannungsfeld zwischen Informationsfreiheit und Datenschutz. Fragen einer bürgerfreundlichen Organisation und Handhabung beider Rechtsgebiete, Möglichkeiten der elektronischen Akteneinsicht sowie Entwicklungsperspektiven der Informationsfreiheit und des Datenschutzes wurden dabei thematisiert. Der internationale Vergleich ermöglichte einen Einblick in unterschiedliche Herangehensweisen zu beiden Themen und trug zu einer differenzierten Einordnung der Praxis des brandenburgischen Akteneinsichtsrechts bei.

Die Teilnehmerzahl war mit 120 Teilnehmerinnen und Teilnehmern bei weitem größer als erwartet. Datenschutzbeauftragte anderer Bundesländer, behördliche Datenschutzbeauftragte aus brandenburgischen Verwaltungen, Interessierte aus der Wissenschaft, Beschäftigte der Behörden und nicht zuletzt interessierte Bürgerinnen und Bürger nahmen an der zweitägigen Veranstaltung in Potsdam teil.

Die Vorträge des Symposiums können aus unserem Internet-Angebot unter http://www.lda.brandenburg.de abgerufen werden.

Kleinmachnow, den 8. März 2000

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht

Anlagen

Anlage 1

Diskussionsgrundlage
zur weiteren Verwendung von Stasi-Unterlagen
zur Überprüfung von Mandatsträgern und Mitarbeiternim öffentlichen Dienst

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. 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 I, 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 abgesehen 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-Unterlagengesetz 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 zu Grunde liegt.

Überprüft wurden in den vergangenen 10 Jahren nahezu ausschließlich Personen aus den neuen Bundesländern, obwohl nach Einschätzung des BStU 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 Stasitätigkeit 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

Tätigkeit 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 Verarbeitung ihrer personenbezogenen Unterlagen durch den Bundesbeauftragten für die Stasi-Unterlagen eingeräumt werden, wenn sie aufgrund 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 betreffenden 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 Staatssicherheitsdienst (§ 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 2

Stellungnahme des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

zum

Grünbuch der Kommission der Europäischen Gemeinschaften über die Informationen des öffentlichen Sektors in der Informationsgesellschaft

KOM (98) 585 endg.; Ratsdok. 5580/99

Es ist zu begrüßen, dass die Europäische Kommission mit der Veröffentlichung des Grünbuchs über die Informationen des öffentlichen Sektors in der Informationsgesellschaft eine unionsweite Diskussion über eine Erweiterung der Zugangsrechte der Bürgerinnen und Bürger zu öffentlichen Informationen initiiert hat. Auch wenn das Grünbuch einen Schwerpunkt auf die kommerzielle Nutzung der Informationen des öffentlichen Sektors legt, hebt es doch zu Recht die Bedeutung des mit dem Vertrag von Amsterdam am 1. Mai 1999 in Kraft getretenen Informationszugangsrechts der Unionsbürger (Artikel 255 des EG-Vertrages in der konsolidierten Fassung) für die Unterstützung des demokratischen Prozesses hervor (Ziffer 21 des Grünbuchs).

Dem entspricht Artikel 21 Abs. 4 der Verfassung des Landes Brandenburg, der im Zusammenhang mit dem Recht auf politische Mitgestaltung jedem nach Maßgabe des Gesetzes das Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen des Landes und der Kommunen garantiert, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen. Dieses Grundrecht auf Informationszugang wird in Brandenburg als erstem Land der Bundesrepublik Deutschland seit dem 20. März 1998 durch das Akteneinsichts- und Informationszugangsgesetz konkretisiert. Nach Maßgabe dieses Gesetzes hat jeder das Recht auf Einsicht in Akten, ohne dass hierfür ein rechtliches oder auch nur berechtigtes Interesse dargetan werden müsste. Allerdings wird das Einsichtsrecht durch zahlreiche Ausnahmetatbestände zu Gunsten überwiegender öffentlicher oder privater Interessen eingeschränkt. Auch wenn das Gesetz in erster Linie dem Ziel der politischen Mitgestaltung dient, können sich auch Bürger oder Unternehmen darauf berufen, die ein kommerzielles Interesse verfolgen, da sie in der Regel nicht verpflichtet sind, ihr Informationsinteresse zu begründen.

Bevor ich zu einzelnen der von der Kommission aufgeworfenen Fragen Stellung nehme, sei eine grundsätzliche Bemerkung zum elektronischen Informationszugang vorangestellt (Ziffer 64, 67 des Grünbuchs). Es besteht kein Zweifel daran, dass die Entwicklung des Internets die Informationszugangsmöglichkeiten für alle erheblich verbessert hat und auch im Verhältnis zu den Informationen der öffentlichen Verwaltung weiter verbessern wird. Das Grünbuch weist zu Recht darauf hin, dass es noch einige Zeit dauern wird, bis dieses Medium für alle zugänglich ist. Aus der Sicht eines Datenschutzbeauftragten, der zugleich Landesbeauftragter für den Informationszugang ist, muss ich aber darauf hinweisen, dass die Möglichkeit eines konventionellen Zugriffs auf Informationen der Verwaltung auch dann erhalten bleiben muss, wenn das Internet für alle zugänglich sein sollte. Die Bürger dürfen nicht gezwungen werden, online mit der Verwaltung zu kommunizieren. Der elektronische Zugriff kann nur eine zusätzliche - sicherlich immer wichtiger werdende - Kommunikationsmöglichkeit für den Bürger sein. Die Zugangsmöglichkeiten zu Informationen der öffentlichen Verwaltung dürfen aber nicht davon abhängig gemacht werden, dass die Bürger über ein bestimmtes technisches Know-how z. B. ein Mindestmaß an Medienkompetenz verfügen.

Zu Frage 1 (Begriff und Arten von Informationen des öffentlichen Sektors):

Die brandenburgische Landesverfassung und das Akteneinsichts- und Informationszugangsgesetz folgen in diesem Punkt sowohl dem funktionalen wie dem gesetzesbasierten/institutionellen Ansatz bei der Begriffsbestimmung des öffentlichen Sektors (Ziffer 72 des Grünbuchs). Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen des Landes und der Kommunen unterliegen dem Zugangsrecht. Dieses Zugangsrecht gilt eingeschränkt für den Landtag, dem Landesrechnungshof, die staatlichen Rechnungsprüfungsämter, die Organe der Rechtspflege und die Hochschulen, soweit sie Verwaltungsaufgaben erledigen. Forschungseinrichtungen, Schulen und Prüfungseinrichtungen müssen Akteneinsicht nur insoweit gewähren, als sie nicht im Bereich von Forschung, Lehre, Unterricht und Prüfung tätig werden.

Grundsätzlich sollte die Kommission bei ihren weiteren Überlegungen alle Arten von Informationen des öffentlichen Sektors mit einbeziehen. Die in den Ziffern 73 ff. des Grünbuchs angesprochenen Differenzierungen lassen sich nicht pauschal treffen, sondern nur aus der Sicht des Bürgers, der Zugang zu den Informationen erhalten will. Ob eine Information unerlässlich für ein funktionierendes demokratischen Gemeinwesen ist oder nicht, kann nicht abstrakt beantwortet werden, sondern hängt von dem Informationsinteresse und der Situation des einzelnen Bürgers ab.

Selbstverständlich können Informationen ohne Personenbezug, etwa Planungsunterlagen, leichter zugänglich gemacht werden als Unterlagen mit Personenbezug, weil nur im zuletzt genannten Fall datenschutzrechtliche Restriktionen zu beachten sind (dazu unten zu Frage 7). Man sollte aber nicht den Fehler begehen, den

Informationszugang von vornherein nur auf nicht personenbezogene Daten zu beschränken, weil dies den Blickwinkel zu sehr verengen und das grundsätzliche Recht auf Informationszugang zu sehr einschränken würde.

Zu Frage 2 (Unterschiedliche Bedingungen für den Informationszugang):

Nach brandenburgischem Landesrecht müssen die Bürger zwar nicht wie in allen anderen Ländern der Bundesrepublik Deutschland ein rechtliches oder berechtigtes Interesse geltend machen, um Zugang zu amtlichen Unterlagen zu erhalten. Soweit jedoch im Land Brandenburg Bundesrecht auszuführen ist, das derartige Restriktionen enthält, geht es dem Brandenburgischen Akteneinsichts- und Informationszugangsgesetz vor. Es gibt zahlreiche unterschiedliche Bedingungen im Bundesrecht für den Informationszugang, die hier nicht im Einzelnen aufgezählt werden sollen. Zweifellos führen diese Bedingungen, vor allem soweit sie mit den Bedingungen in den übrigen Mitgliedstaaten der Europäischen Union nicht übereinstimmen, zu Hindernissen für den Informationszugang auf europäischer Ebene. Insofern bildet die Bundesrepublik Deutschland gemeinsam mit Großbritannien und Luxemburg das Schlusslicht der europäischen Rechtsentwicklung hinsichtlich des allgemeinen Informationszugangsrecht (vgl. Anhang 1 des Grünbuchs), weil auf bundesrechtlicher Ebene ein allgemeines Informationszugangsgesetz bisher fehlt.

Es wäre deshalb zu begrüßen, wenn die Kommission die notwendigen Schritte zur Rechtsangleichung auf europäischer Ebene unternehmen würde, um die skizzierten unterschiedlichen Zugangsbedingungen durch den Erlass einer Richtlinie zum allgemeinen Informationszugang zu harmonisieren.

Zu Frage 3 (Informationen über die verfügbaren Daten):

Ich halte die Zusammenstellung von Metadaten (Informationen über die verfügbaren Daten) für eine entscheidende Voraussetzung dafür, dass das Datenangebot des öffentlichen Sektors besser genutzt werden kann. Ich setze mich deshalb im Land Brandenburg dafür ein, dass in einem ersten Schritt die Behörden und Einrichtungen des Landes für ihren jeweiligen Bereich Aktenpläne aufstellen und allgemein (möglichst im Internet) publizieren. Dasselbe gilt für elektronische Datenbestände.

Zugleich sollten die öffentlichen Stellen von sich aus verstärkt Informationsangebote für die Bürger machen und benutzerfreundliche Suchfunktionen sowohl konventionell als auch elektronisch zur Verfügung stellen.

Ein wichtiger Punkt in diesem Zusammenhang ist auch die notwendige Umstrukturierung der Informationsbestände, um den Informationszugang zu erleichtern. Das novellierte Brandenburgische Datenschutzgesetz vom 21. Dezember 1998 (Bekanntmachung der Neufassung vom 9.3.1999, GVBl. I S. 66), das der Umsetzung der Richtlinie 46/95/EG dient, enthält erstmals eine Vorschrift über die Organisation der Datenverarbeitung, nach der eine Trennung der Daten in den einzelnen Verarbeitungsphasen nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich sein muss. Insbesondere auch die Trennung zwischen personenbezogenen und nicht personenbezogenen Aktenteilen oder Datenbanksegmenten ist geeignet, den Informationszugang für Dritte zu erleichtern oder überhaupt erst zu ermöglichen. Der Aspekt der Informationszugangsfreundlichkeit muss in Zukunft bei der Organisation von konventionellen und elektronischen Datenbeständen stärker berücksichtigt werden.

Zu Frage 4 (Kosten des Informationszugangs):

Die „Preispolitik“ im Sinne der Fragestellung spiegelt sich in den Kostenregelungen des nationalen Rechts wider. Unterschiede in diesen Regelungen führen zwangsläufig auch zu Unterschieden in der nationalen und europaweiten Zugänglichkeit von Informationen. Prinzipiell wirkt jede Kostenpflicht beim Informationszugang als Hindernis. Deshalb kommt dem elektronischen Informationszugang so große Bedeutung zu, weil bei ihm die Kosten des Informationsabrufs stark zurückgehen oder sogar ganz entfallen. Aber auch soweit es um den konventionellen Informationszugang (Einsicht in Akten etc.) geht, ist es wichtig, dass national wie auch auf europäischer Ebene nicht die gesamten Kosten der Informationsbereitstellung und des Informationszugangs auf den Informationsinteressenten abgewälzt werden dürfen. Das Brandenburgische Akteneinsichts- und Informationszugangsgesetz enthält eine Kostenregelung, nach der die Gebühren so zu bemessen sind, dass zwischen dem Verwaltungsaufwand einerseits und dem Grundrecht auf Akteneinsicht andererseits ein angemessenes Verhältnis besteht. Die Landesregierung hat die erforderliche Gebührenordnung hierzu allerdings noch nicht erlassen.

Überlegungen, wie sie im Grünbuch aus anderen Rechtsordnungen referiert werden, die Preise danach zu differenzieren, ob die gewünschten Informationen zur Wahrnehmung der demokratischen Rechte „wesentliche Bedeutung für den Bürger“ haben oder nicht, erscheinen als problematisch. Zum einen widerspricht es einer allgemeinen Informationszugangsgesetzgebung, den Bürger zu einer Begründung seines Informationsinteresses zu veranlassen. Zum anderen müsste sichergestellt werden, dass Informationen, die zunächst für einen „preiswerten“ Zweck abgefragt worden sind, nicht anschließend für einen „teureren“ (kommerziellen) Zweck weiter verwendet werden.

Zu Frage 7 (Datenschutz):

Zu Recht hebt das Grünbuch (Ziffer 110) hervor, dass es sich nur bei einem Teil der Informationen des öffentlichen Sektors um personenbezogene Daten handelt. Allerdings ist gerade dieser Teil von besonderem Interesse für bestimmte Unternehmen, die z. B. im Bereich der Direktwerbung tätig sind. Insofern verdienen Datenschutzfragen im Zusammenhang mit der Nutzung von Informationen des öffentlichen Sektors in der Tat besondere Aufmerksamkeit. Die im Grünbuch (III Pkt. 7) enthaltenen Formulierungen deuten demgegenüber darauf hin, dass dem Schutz der Privatsphäre des Einzelnen im Verhältnis zum Informationsrecht der Bürger und der Unternehmen ein zu geringer Stellenwert eingeräumt wird. So wird von der Notwendigkeit gesprochen, das Informationszugangsrecht und das Recht auf Schutz der Privatsphäre gegeneinander abzuwägen, was in allen einzelstaatlichen Zugangsregelungen vorgesehen sei.

Das Brandenburgische Akteneinsichts- und Informationszugangsgesetz macht demgegenüber die Einsichtnahme in personenbezogene Unterlagen der öffentlichen Verwaltung (soweit sie Daten anderer Bürger und nicht nur der Verwaltungsmitarbeiter enthalten) von der ausdrücklichen Einwilligung der Betroffenen abhängig. Ohne Einwilligung kann in amtliche Unterlagen mit Personenbezug nur dann Einsicht genommen werden, wenn auf Grund besonderer Umstände des Einzelfalls im Hinblick auf den Zweck der politischen Mitgestaltung das Offenbarungsinteresse des Antragsstellers das Interesse der betroffenen Person an der vertraulichen Behandlung der Information überwiegt. Nur das Mitgestaltungsinteresse der Bürger kann also im Einzelfall dazu führen, dass auf Grund einer Abwägung das Interesse des betroffenen Einzelnen am Schutz seiner Privatsphäre zurücktreten muss. Das kommerzielle Verwertungsinteresse von Bürgern oder Unternehmen kann den Schutz der Privatsphäre dagegen nicht zurückdrängen oder aufheben. Das entspricht auch der verfassungsrechtlichen Grundsituation im Land Brandenburg wie in der Bundesrepublik Deutschland insgesamt, wonach Eingriffe in das informationelle Selbstbestimmungsrecht der Bürger nur im überwiegenden Interesse der Allgemeinheit zulässig sind.

Auch das Europäische Parlament und der Rat haben in der Richtlinie 97/66/EG (Telekommunikations-Datenschutz) vom 15. Dezember 1996 (ABl. EG L 24/1) für einen speziellen Bereich festgelegt, dass Betreiber von Telekommunikationsdiensten bestimmte personenbezogene Daten nur mit Einwilligung der Teilnehmer zum Zwecke der Vermarktung verarbeiten dürfen.

Darin kommt eine grundlegende Wertung zum Ausdruck, die auch beim allgemeinen Zugang zu Informationen der öffentlichen Verwaltung nicht aufgegeben werden sollte: Wirtschaftliche Interessen allein rechtfertigen es nicht, die informationelle Selbstbestimmung des Einzelnen zu übergehen. Dies gilt insbesondere für den Zugang zu sensiblen personenbezogenen Daten wie medizinischen Informationen, Arbeitnehmerdaten und Sozialdaten.

Lediglich am Rande sei bemerkt, dass das Statistikgeheimnis nicht nur den Schutz personenbezogener Daten verstärkt, sondern auch die vertrauliche Behandlung von statistischen Informationen mit Bezug auf einzelne Unternehmen vorschreibt (vgl. Ziffer 113).
Von besonderer Bedeutung ist die Einhaltung des Zweckbindungsprinzips, das in der Richtlinie 95/46/EG vom 24. Oktober 1995 verankert worden ist. Auch wenn personenbezogene Daten in zulässiger Weise für die Allgemeinheit zugänglich gemacht werden, darf dies nicht dazu führen, dass diese Daten ohne jede Zweckbindung genutzt und vom Anwendungsbereich der Datenschutzgesetze völlig freigestellt werden. Es bleiben personenbezogene Daten, auf deren Verwendung der betroffene Bürger weiterhin entscheidenden Einfluss nehmen kann. Er muss auch die Möglichkeit behalten, ihre Verwendung zu bestimmten Zwecken, die seine schutzwürdigen Belange tangieren, zu unterbinden. So kann auch nach brandenburgischem Landesrecht der betroffene Bürger seine Einwilligung in die Akteneinsicht durch Dritte widerrufen.

Datenschutz und allgemeiner Informationszugang bilden keinen unauflöslichen Gegensatz. Für die notwendige Verzahnung beider Gesichtspunkte in der Praxis müssen allerdings weitergehende Überlegungen angestellt werden, als dies im Grünbuch bisher geschehen ist. Insbesondere muss einer Entwicklung vorgebeugt werden, bei der das Datenschutzrecht seine Geltung verliert, sobald personenbezogene Daten allgemein zugänglich gemacht worden sind. Datenschutz- und Informationszugangsrecht stehen nicht trennscharf nebeneinander, sondern überlagern sich. Informationelle Selbstbestimmung des einzelnen Betroffenen endet nicht in dem Augenblick, in dem Daten über ihn öffentlich verfügbar gemacht worden sind.

Im Übrigen können auch technische Beschränkungen des Informationszugangs (quantitative Beschränkungen, Rechercherestriktionen) unter Umständen den Schutz der Privatsphäre des Einzelnen mit den Informationsinteressen der Allgemeinheit in Einklang bringen.

Zu Frage 9 (Aktivitäten der Europäischen Union):

Die Europäische Union sollte die Umsetzung der Transparenzvorschriften des Vertrags von Amsterdam (insbesondere Artikel 255) konsequent vorantreiben. In diesem Zusammenhang sollte auch die Errichtung einer unabhängigen Kontrollinstanz für den Informationszugang in den Institutionen der Europäischen Union geprüft werden, wie sie für den Datenschutz in Artikel 286 Abs. 2 EGV vorgesehen, allerdings noch nicht errichtet worden ist. Angesichts des engen Zusammenhangs zwischen den Fragen des allgemeinen Informationszugangs und des Datenschutzes liegt es nahe, beide Aufgaben einer gemeinsamen Kontrollinstanz zu übertragen. Die bisherigen Erfahrungen im Land Brandenburg haben zum einen gezeigt, dass eine unabhängige Instanz als Adressat für

Bürgerbeschwerden eine wichtige Voraussetzung zur Umsetzung der Regelungen zum Informationszugang ist. Zum anderen hat sich die Entscheidung des Landesgesetzgebers bewährt, diese Aufgabe dem Landesbeauftragten für den Datenschutz entsprechend dem Vorbild in zahlreichen kanadischen Provinzen und in Ungarn zu übertragen. Auf diese Weise werden Reibungsverluste zwischen den für den Datenschutz und für den Informationszugang zuständigen Instanzen vermieden.

Zu Frage 10 (Vorrang der Handlungsfelder):

Angesichts der unterschiedlichen Rechtslage in den Mitgliedstaaten der Union sollte die Kommission den Entwurf einer Richtlinie zum allgemeinen Informationszugang erarbeiten, um auf diese Weise zu einem harmonisierten europäischen Mindeststandard zu gelangen. Zudem sollten vorrangig Demonstrations- und Pilotvorhaben zur Verbreitung von Technologien für den elektronischen Zugang zu Informationen im öffentlichen Sektor unterstützt werden.

Auch die anderen in Ziffer 123 genannten Handlungsfelder sind in diesem Zusammenhang von Bedeutung.
Ich verweise außerdem auf die Stellungnahme der Gruppe nach Artikel 29 der Richtlinie 46/95/EG, die diese zum Grünbuch erarbeitet hat und die ich unterstütze.

Dieser Stellungnahme ist unser Tätigkeitsbericht 1998 beigefügt, der zu einzelnen Fragen des Informationszugangs im öffentlichen Bereich nähere Ausführungen enthält. Er ist zudem - ebenso wie der Text des Akteneinsichts- und Informationszugangsgesetzes und des Brandenburgischen Datenschutzgesetzes - im Internet (nur in deutscher Sprache) abrufbar.

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg

Anlage 3

Auszug aus dem Geschäftsverteilungsplan des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Stand: 31. Dezember 1999

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix
Stellvertreter	Kurt Urban
Mitarbeit bei: - Akteneinsicht und Informationszugang - Verwaltungsmodernisierung - Redaktion von Veröffentlichungen	Dipl. Verwaltungswissenschaftler Sven Müller App. 20
Sekretariat	Christine Objartel App. 10

Bereich Recht

Bereichsleiter	Dr. Frank Jendro App. 34
Arbeitsgebiete: - Rechtliche Grundsatzfragen - Landtag, Staatskanzlei - Justiz (außer Staatsanwaltschaften) - Finanzen - Landesrechnungshof - Beauftragter des Haushalts	
Arbeitsgebiete:	Lena Schraut

- Inneres (insbes. Polizei, Verfassungsschutz, Verkehrsordnungswidrigkeiten, Ausländer, Asylverfahren) - Staatsanwaltschaften - Presse- und Öffentlichkeitsarbeit	App. 41
Arbeitsgebiete: - Arbeit, Soziales, Gesundheit, Frauen - Sozial- und Gesundheitsdaten allgemein	Marion Bultmann App. 44
Arbeitsgebiete: - Inneres (insbes. Melderecht, Kommunalrecht, Personenstandsrecht, Einbürgerung, Wahlen) - Personaldaten allgemein - Telekommunikation und Medien	Sven Hermerschmidt App. 40
Arbeitsgebiete: - Bildung, Jugend, Sport - Wissenschaft, Forschung, Kultur	Gabriele Peschenz App. 22
Arbeitsgebiete: - Landwirtschaft, Umweltschutz, Raumordnung - Wirtschaft, Mittelstand, Technologie - Stadtentwicklung, Wohnen, Verkehr	Susann Burghardt App. 45
Arbeitsgebiete: - Personal- und Verwaltungsangelegenheiten des LDA - Büroleitungsaufgaben - Haushaltsangelegenheiten-	Dipl.-Betriebswirtin (FH) Ursel Leunig App. 42 Beschaffungen allgemein
Arbeitsgebiete: - Bibliothek - Literaturbeschaffung - Schreibdienst	Dipl.-Bibliothekarin (FH) Christel Kern App. 43

- Informationsmaterialien

Bereich Technik

Bereichsleiter	Kurt Urban App. 30
Arbeitsgebiete: - Technisch/organisatorische Grundsatzfragen - Landesverwaltungsnetz - komplexe IT-Verfahren	
Arbeitsgebiete: - Großrechner - Datenbanksysteme - kryptographische Verfahren - Organisations-/ Dienstanweisungen - Statistik - Beratung der behördlichen Datenschutzbeauftragten und Personalräte	Ulrich Wiener App. 31
Arbeitsgebiete: - UNIX-Systeme - Sicherheitsprodukte - Kartentechnologien - Kommunikationsnetze - Telekommunikation und Medien	Dipl.-Ingenieur für Informationstechnik Veikko Müller App. 32
Arbeitsgebiete: - Systemverwalter - Gebäudesicherung - Datenträgerentsorgung - Isolierte und vernetzte PC	Dipl.-Ingenieur (FH) Udo Thiele App. 33

Arbeitsgebiete: - Teilaufgaben der autom. Vorgangsverwaltung - Mailboxkommunikation mit BfD, LfDen - Schreibdienst - Informationsmaterialien	Dipl. Betriebswirtin (FH) Gabriela Berndt App. 12
Gleichstellungsbeauftragte	Frau Kern App. 43
Personalrat	Herr Wiener App. 31
Behördlicher Datenschutzbeauftragter	Herr Hermerschmidt App. 40

Anlage 4

Aktenplan des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Problemkreis	Bezeichnung
002	Akteneinsichts- und Informationszugangsgesetz
003	Arbeit
008	Ausländer
009	Bau-/Wohnungswesen
010	Landesregierung
024	Landtag/Parteien
027	Bildung/Kultur/Wissenschaft
028	BRD/Bund/Bundesländer
034	Allgemeines Datenschutzrecht
046	Zusammenarbeit Bundesbeauftragter für den Datenschutz/Landesbeauftragte für den Datenschutz
054	Dateienregister LDA
056	Internationale Datenschutzangelegenheiten
061	Finanzen
062	Ernährung/Landwirtschaft/Forsten
066	Gesundheitswesen
078	Familie/Frauen/Jugend
082	Justiz
086	Kommunalrecht
089	Interne Verwaltung LDA
100	Öffentlichkeitsarbeit LDA
104	Inneres

108	Personaldatenverarbeitung
110	Polizei
128	Sozialwesen
132	Statistik
135	Technik
136	Medien/Telekommunikation/Post
138	Umwelt/Raumordnung/Stadtentwicklung
146	Verfassungsschutz
147	Verkehr
154	Wirtschaft/Technologie
163	Nicht-öffentlicher Datenschutz
180	Personalräte
999	Sonstiges

Abkürzungsverzeichnis

a. a. O.	=	am angegebenen Ort
ABl.	=	Amtsblatt
ABM	=	Arbeitsbeschaffungsmaßnahme
Abs.	=	Absatz
ADV	=	automatische Datenverarbeitung
AIG	=	Akteneinsichts- und Informationszugangsgesetz
Anl.	=	Anlage
AO	=	Abgabenordnung
APIS	=	Arbeitsdatei "PIOS - Innere Sicherheit"
APSIS	=	Automatisierte Personalvertretung und Stellenbewirtschaftung im Schulamt
Art.	=	Artikel
Az.	=	Aktenzeichen
BArchG	=	Bundesarchivgesetz
Bbg.	=	Brandenburgisch(es)
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgBO	=	Brandenburgische Bauordnung
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BDSG	=	Bundesdatenschutzgesetz
BGBl.	=	Bundesgesetzblatt
BIS	=	Brandenburger InformationsStrategie
BKAG	=	Bundeskriminalamtsgesetz
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
bzgl.	=	bezüglich
bzw.	=	beziehungsweise
c't	=	ct magazin für computertechnik
CD-ROM	=	Compact Disc - Read Only Memory
d. h.	=	das heißt
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg

DDR	=	Deutsche Demokratische Republik
DNA	=	desoxyribonucleic acid (deutsch: Desoxyribonucleinsäure)
DSV	=	Datenschutzverordnung Schulwesen
DuD	=	Datenschutz und Datensicherheit
DVBl.	=	Deutsches Verwaltungsblatt
DVU	=	Deutsche Volksunion
e. V.	=	eingetragener Verein
EDV	=	Elektronische Datenverarbeitung
EG	=	Europäische Gemeinschaft
endg.	=	endgültig
etc.	=	et cetera
EU	=	Europäische Union
EuGH	=	Europäischer Gerichtshof
EuGRZ	=	Europäische Grundrechtszeitschrift
evtl.	=	eventuell
FAZ	=	Frankfurter Allgemeine Zeitung
ff.	=	folgende
G 10-Gesetz	=	Gesetz zu Artikel 10 Grundgesetz
geänd.	=	geändert
gem.	=	gemäß
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GmbH	=	Gesellschaft mit beschränkter Haftung
GO	=	Gemeindeordnung
GVBl.	=	Gesetz- und Verordnungsblatt
HKR	=	Haushalt-, Kassen-, Rechnungswesen
i. d. Fass.	=	in der Fassung
i. d. R.	=	In der Regel
i. S. d.	=	im Sinne des
i. S. v.	=	im Sinne von
i. V. m.	=	in Verbindung mit
INPOL	=	Informationssystem der Polizei
IP	=	Internet-Protokoll
IT	=	Informationstechnik

JuMiG	=	Justizmitteilungsgesetz
KAN-BB	=	Kriminalaktennachweis Land Brandenburg
Kfz	=	Kraftfahrzeug
KHDsV	=	Verordnung zum Schutz von Patientendaten im Krankenhaus
KHG	=	Krankenfinanzierungsgesetz
KOM	=	Dokument der Europäischen Kommission
KPMD	=	kriminalpolizeiliches Meldesystem
LAN	=	(Local Area Network) Landesverwaltungsnetz
LDA	=	Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
LDS	=	Landesamt für Datenverarbeitung und Statistik
LHO	=	Landeshaushaltsordnung
LKV	=	Landes- und Kommunalverwaltung
LRHG	=	Landesrechnungshofgesetz
LT-Drs.	=	Landtags-Drucksache
LVerfG	=	Landesverfassungsgericht
LVN	=	Landesverwaltungsnetz
NJW	=	Neue Juristische Wochenschrift
Nr.	=	Nummer
o. g.	=	oben genannte
o. Ä.	=	oder Ähnliches
OECD	=	Organization Economic Cooperation and Developtment (deutsch: Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
ORB	=	Ostdeutscher Rundfunk Brandenburg
PC	=	Personalcomputer
PERIS	=	Personalinformationssystem der Landesverwaltung
PersVG	=	Personalvertretungsgesetz für das Land Brandenburg
PGP	=	Pretty Good Privacy
PIN	=	persönliche Kennzahl
PISA	=	Programm for International Student Assessment
Pkt.	=	Punkt
POGBbg	=	Polizeiorganisationsgesetz
RSA	=	Verschlüsselungsalgorithmus nach den Entwicklern Rivest, Shamir und Adleman
s. o.	=	siehe oben
s.	=	siehe
S.	=	Seite

SGB	=	Sozialgesetzbuch
SGB I	=	Erstes Buch Sozialgesetzbuch
SGB V	=	Fünftes Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
sog.	=	sogenannt
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
TK	=	Telekommunikation
TV	=	Television
u. a.	=	unter anderem
u. Ä.	=	und Ähnliches
UIG	=	Umweltinformationsgesetz
US	=	United States
USA	=	United States of America
u. U.	=	unter Umständen
VfGBbg	=	Verfassungsgericht des Landes Brandenburg
VG	=	Verwaltungsgericht
vgl.	=	vergleiche
VO	=	Verordnung
VSK	=	Verwaltungsstrukturkommission
VwGO	=	Verwaltungsgerichtsordnung
VwVfG	=	Verwaltungsverfahrensgesetz
WWW	=	World Wide Web
z. B.	=	zum Beispiel
z. T.	=	zum Teil
zz.	=	zurzeit

Dokumente

zum Datenschutz

1999

A. Beschlüsse und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

I. Entschließungen der 57. Konferenz am 25./26. März 1999 in Schwerin

Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein "Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutz-verordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die

Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Transparente Hard- und Software

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation

(ENFOPOL '98)

(Entschließung der 57.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL '98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

II. Entschließungen zwischen den Konferenzen 1999

Angemessener Schutz auch für Untersuchungsgefangene

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. August 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lässt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

- Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

- Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelener Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.
- Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

- Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z. B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

- Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

"Gesundheitsreform 2000"

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1999)

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes "Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiter reichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

I. Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

II. Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

III. Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

IV. Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

V. Die zur Begründung besonders angeführten Punkte "Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern" vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

VI. Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

VII. Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Juni 1999)

Bei der Einführung der Befugnis zum „Großen Lauschangriff" hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weit reichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz hervor. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

III. Entschließungen der 58. Konferenz am 7./8. Oktober 1999 in Rostock

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

"Täter-Opfer-Ausgleich und Datenschutz"

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbe-sondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestim-mung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat viel-mehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des "Täter-Opfer-Ausgleichs" nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als "objektive Dritte mit dem Gebot der Unterstützung jeder Partei" könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die "fachlich geleitete Auseinandersetzung" der "am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden".

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am "Täter-Opfer-Ausgleich" Beteiligten muss gesetzlich geschützt werden.

Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garan-tien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwie-genden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Ne-ben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunika-tion und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,

- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,

- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),

- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,

- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: "Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs.1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs.1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Patientenschutz durch Pseudonymisierung

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. 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.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, be-dürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststel-lungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne richterliche Anordnung - erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über

Vollzugslockerungen nicht beeinflusst, ist den-noch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informati-onstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weit reichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern stattdessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100a StPO neu geregelt werden.

B. Datenschutzbeauftragte fordern Trendwende in der Telekommunikationspolitik: Weg vom Anspruch auf lückenlose Überwachung hin zu einem effektiven Schutz des Fernmeldegeheimnisses

Berliner Datenschutzbeauftragter

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Der Landesbeauftragte für den Datenschutz freie Hansestadt Bremen

Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Der Landesbeauftragte für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages

Für eine Sicherung der freien Telekommunikation in unserer Gesellschaft

Hintergrundpapier

Inhaltsübersicht

8. Erweiterte Rolle der "Dienste"

III. Forderungen

1. Gesetz zur Sicherung der freien Telekommunikation erlassen
2. "Mediennutzungsgeheimnis" einführen
3. Überwachungspflichten begrenzen
4. Effektivität kontrollieren
5. Illegales Abhören stärker sanktionieren
6. Berufliche Schweigepflichten garantieren
7. Kommunikationsgeheimnis auch strafrechtlich besser schützen

I. Telekommunikation boomt - Grundrechte gefährdet

Die Bedeutung der Telekommunikation hat in den letzten Jahrzehnten stark zugenommen und dieser Trend wird sich weiter beschleunigen. Seit der Erfindung des "Fernsprechers" in der zweiten Hälfte des 19. Jahrhunderts sind weltweite Telekommunikationsnetze entstanden, deren Bedeutung sich grundlegend gewandelt hat. Über diese Netze wird längst nicht mehr nur Sprache transportiert, sondern auch Telefaxe (vom Telex oder "Fernschreiber" spricht heute kaum noch jemand) und Informationen aller Art in digitalisierter Form (bis hin zu Bildern, Musikstücken etc.). Mit Hilfe der Telekommunikation können Entfernungen zwischen Kontinenten z.B. satellitengestützt in Sekundenschnelle überbrückt und lebenswichtige Informationen in kürzester Zeit an den Zielort übermittelt werden. Das Internet, das zugleich die *Konvergenz von Individual- und Massenkommunikation*, von Telekommunikation, Fernsehkonsum und Multimedia verdeutlicht, ist nur die vorläufig letzte Stufe der Entwicklung von Telekommunikationsnetzen. Nicht ohne Grund widmet die *Internationale Funkausstellung Berlin 1999* dem Internet besondere Aufmerksamkeit. Die Menschen "unterhalten" sich in mehrfacher Hinsicht mit Hilfe der Telekommunikation. Digitalfernsehen, Web-TV und Push-Technologien einerseits und die bevorstehende Nutzung von Kabelnetzen für Sprachtelefonie andererseits lassen die Grenzen zwischen Fernseh- und PC-Nutzung zunehmend verschwimmen. Fest- und Mobilfunknetze wachsen immer mehr zusammen. Die Informationsgesellschaft ist ohne Telekommunikation undenkbar.

Die medial vermittelte Kommunikation ergänzt zunehmend neben die unmittelbare Kommunikation zwischen Menschen, ohne sie völlig ersetzen zu können. Patientinnen und Patienten holen telefonisch ärztlichen Rat ein,

Menschen in seelischer Not nutzen die Telefonseelsorge oder die Drogenberatung im Internet, Wirtschaftsunternehmen tauschen Daten miteinander aus. Umso wichtiger ist es, dass die Kommunikation unter Einschaltung der Technik, die Dritte zur Verfügung stellen, ebenso *vertraulich* stattfinden kann wie die unmittelbare persönliche Kommunikation (jedenfalls wenn - was der Regelfall ist - alle Beteiligten dies wünschen). Dem dient das grundrechtlich geschützte *Fernmelde- oder Telekommunikationsgeheimnisgeheimnis (Art. 10 Grundgesetz).* Es soll eine *überwachungsfreie Kommunikation* sichern und ist von zentraler Bedeutung nicht nur für den Grundrechtsschutz der einzelnen Bürgerinnen und Bürger, sondern auch für die freie Kommunikation in einer freien und demokratischen Gesellschaft insgesamt. Denn "...die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen, hier insbesondere zur Vermeidung bestimmter Gesprächsinhalte...führen." Diese Umstände, die das Bundesverfassungsgericht in seiner jüngsten Entscheidung zur *verdachtslosen Rasterfahndung* im grenzüberschreitenden Fernmeldeverkehr (BVerfG, Urt, v. 14.7.1999, - 1 BvR 2226/94 - u.a., S. 95) ausdrücklich hervorgehoben hat, sind bisher zu wenig beachtet worden.

II. Kontrollnetz wird immer engmaschiger

Dem Telekommunikationsgeheimnis (Artikel 10 Grundgesetz) droht durch die technischen und rechtlichen Entwicklungen eine *Erosion*, der dringend Einhalt geboten werden muss, wenn die Informationsgesellschaft in Deutschland eine demokratisch und rechtsstaatlich verantwortbare Zukunft haben soll.

Staatliche Überwachungsmaßnahmen in offenen Kommunikationsnetzen berühren angesichts des sich abzeichnenden Wandels des Internets zum Massenmedium zugleich die grundrechtlich geschützte Freiheit, frei die eigene Meinung zu äußern *(Meinungsfreiheit, Artikel 5 Abs.1 Satz 1 Grundgesetz)* und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten *(Informationsfreiheit, Artikel 5 Abs.1 Satz 1 Grundgesetz).* Müssten Internet-Nutzerinnen und -Nutzer stets damit rechnen, dass sie vom Staat beobachtet werden, würde dies ihre Informationsfreiheit beeinträchtigen. Strafbare Inhalte, die im Internet angeboten werden, müssen an der Quelle, also bei denjenigen verfolgt werden, die diese Inhalte ins Netz stellen. Keinesfalls rechtfertigt es die *Strafverfolgung im Internet*, den gesamten Netzverkehr, also insbesondere das Verhalten der Nutzerinnen und Nutzer flächendeckend zu überwachen.

1. Datenspuren überall

Aufgrund der *Digitalisierung der Telekommunikationsnetze* hinterlässt jede Nutzung (jedes Telefongespräch, Fax, E-Mail, jeder Abruf aus dem WorldWideWeb) personenbezogene Spuren, die - für die Dauer ihrer Speicherung - ausgewertet werden können. In den gegenwärtig existierenden Mobilfunknetzen werden die Teilnehmerinnen und Teilnehmer "geortet", um die Verbindung herstellen zu können. Die Technik erlaubt die Erstellung von *Bewegungsprofilen*. Es gibt zwar zahlreiche Vorschläge aus der Wissenschaft für eine datenschutzfreundlichere Verbindungstechnik, sie konnten sich aber bisher - auch in der internationalen Standardisierung - nicht durchsetzen. Insofern ist das in der Bundesrepublik inzwischen flächendeckend eingeführte digitale Telekommunikationsnetz im Gegensatz zum früheren analogen Telefonnetz eine Infrastruktur, die eine *intensivere Überwachung* der Nutzerinnen und Nutzer technisch ermöglicht.

2. Immer mehr staatliche Abhörbefugnisse

Die materiell-rechtlichen *Befugnisse zur Überwachung* des Fernmeldeverkehrs durch Nachrichtendienste und Strafverfolgungsbehörden sind seit Verabschiedung der Notstandsgesetze 1968 *ständig ausgedehnt* worden. Allein der Katalog der Straftatbestände in der Strafprozessordnung, zu deren Verfolgung die Telekommunikation überwacht werden darf, ist 17-mal direkt erweitert worden. Zudem haben die Verfassungsschutzämter des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst für geheimdienstliche Zwecke sogar schon im *Vorfeld konkreter Gefahren* und seit 1994 auch das Zollkriminalamt zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz und dem Kriegswaffenkontrollgesetz das Recht, die Telekommunikation zu überwachen. Damit aber nicht genug: Es gibt kaum ein gesellschaftliches Problem *vom Doping bis zur Korruption*, zu dessen Bekämpfung nicht nach einer weiteren Ausdehnung der Abhörbefugnisse gerufen wird.

3. Effektivitätskontrolle? Fehlanzeige!

Bei der ständigen Erweiterung der Abhörbefugnisse fällt eines auf: Wenn darin ein unverzichtbares Mittel zur Bekämpfung aller möglichen Kriminalitätsformen oder auch nur gesellschaftlich unerwünschten Verhaltens gesehen wird, könnte angenommen werden, dass die Effektivität dieses Mittels hinreichend belegt ist. Das Gegenteil ist der Fall. *Aussagekräftige Statistiken oder eine Rechtstatsachenforschung zur Wirksamkeit der Fernmeldeüberwachung fehlen bisher fast völlig oder ihre Ergebnisse werden geheim gehalten*. Dies deutet darauf hin, dass die Sicherheitsbehörden insgesamt gesehen kein Interesse an einer empirischen Überprüfung und objektiven Qualitätskontrolle der ausgedehnten Überwachungsbefugnisse haben, sondern eine öffentliche Diskussion dieser Frage eher scheuen. Zwar hat die Bundesregierung jetzt erklärt, dass die Wirksamkeit der strafprozessualen Fernmeldeüberwachung erstmals Gegenstand eines Forschungsprojekts sein soll. Der Evaluationsansatz muss allerdings sehr viel umfassender sein.

Auch fehlen Zahlen über die Häufigkeit, mit der Gerichte entsprechenden Anträgen der Sicherheitsbehörden folgen bzw. sie ablehnen. Deshalb lässt sich keine Aussage darüber treffen, ob der sog. *Richtervorbehalt* als verfahrensmäßige Sicherung gegenüber Telefonüberwachungsmaßnahmen in Strafverfahren überhaupt eine nennenswerte (sichernde) Filterfunktion ausübt. Dem steht die Praxis in den Vereinigten Staaten gegenüber, wo - übrigens vom Volk gewählte - Richterinnen und Richter über die Zahl und Wirksamkeit der von ihnen erlassenen Abhöranordnungen regelmäßig in öffentlichen Berichten *(wiretap reports)* Rechenschaft ablegen müssen.

Die wenigen vorliegenden Informationen zeigen allerdings zweierlei: Die Zahl der Überwachungsanordnungen hat in den vergangenen Jahren deutlich zugenommen (bundesweit wurden 1997 mehr als doppelt so viel Überwachungen angeordnet als 1995). Zum anderen wird deutlich, dass sich *Überwachungsmaßnahmen* keineswegs nur gegen Verdächtige, sondern mindestens genauso oft *gegen unverdächtige Dritte* richten, mit denen oder von deren Anschluss aus die Verdächtigen nach Ansicht der Ermittlungsbehörden telefonieren könnten. Jede Überwachungsmaßnahme in Kommunikationsnetzen erstreckt sich zwangsläufig auch auf andere Personen als nur die Verdächtigen. Wer aber weiss schon, dass die Telefonverbindung mit einer Person besteht, gegen die wegen einer bestimmten Straftat ermittelt wird?

4. Betrieb von Telekommunikationsnetzen verpflichtet zur geheimen Zuträgerschaft

Neben der Ausweitung der materiell-rechtlichen Überwachungsbefugnisse hat der Gesetzgeber in den letzten Jahren zahlreiche Vorschriften erlassen, die die *lückenlose technische Überwachbarkeit der Telekommunikation* möglichst

unter allen Umständen und insbesondere auch in einem liberalisierten Telekommunikationmarkt sicherstellen sollen.

So verpflichtet die *Fernmelde-Überwachungsverordnung* von 1995 jede Person, die eine für den *öffentlichen Verkehr* bestimmte Fernmeldeanlage betreibt, angeordnete Überwachungsmaßnahmen mit entsprechenden technischen Schnittstellen umzusetzen und dabei nicht nur den Inhalt der übermittelten Nachrichten unverschlüsselt bereitzustellen, sondern auch Informationen über *die näheren Umstände der Telekommunikation*, also die angerufene Zielnummer, Beginn und Ende der Verbindung oder des Verbindungsversuchs, Art des genutzten Dienstes und bei Mobilfunkanschlüssen auch die Funkzellen (die Standorte), über die die Verbindung abgewickelt wird.

Auch das *Telekommunikationsgesetz* von 1996 verpflichtet alle, die Telekommunikationsanlagen (bisher: Fernmeldeanlagen) betreiben, angeordnete Überwachungsmaßnahmen jederzeit umzusetzen. Dabei sind unter Telekommunikationsanlagen nach der weiten gesetzlichen Definition alle "technischen Einrichtungen oder Systeme" zu verstehen, "die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können."

Der 11. Teil des Telekommunikationsgesetzes regelt sowohl das Fernmeldegeheimnis als auch die Pflicht zur Beteiligung an Überwachungsmaßnahmen. Zu Recht hat der Gesetzgeber den Anwendungsbereich des Fernmeldegeheimnisses nach dem Wegfall des Postmonopols auf alle Unternehmen und Personen erstreckt, die Telekommunikationsdienste erbringen, um die Vertraulichkeit der Telekommunikation auch in einem liberalisierten Markt auf demselben Niveau zu gewährleisten wie bisher. Dass der Gesetzgeber aber in diesem Zusammenhang im gleichen Atemzug auch *alle, die geschäftsmäßig Telekommunikation anbieten*, also selbst diejenigen, die *Nebenstellenanlagen* z. B. in *Krankenhäusern und Hotels* betreiben, zur Umsetzung von Überwachungsmaßnahmen verpflichtet, führt zu einem weit über den bisherigen Zustand unter Monopolbedingungen hinausreichenden Grad an Überwachbarkeit und ist unverhältnismäßig. Erfasst werden nun alle, die Telekommunikationsanlagen betreiben; ausreichend ist z. B. schon, dass in einem Betrieb oder einer Behörde den Mitarbeiterinnen und Mitarbeitern erlaubt wird, die Nebenstellenanlage oder das interne Netz auch für private Zwecke zu nutzen. Die Nebenfolge dieser Bestimmung ist nicht nur, dass die genannten Stellen ihre Telekommunikationsanlage nur in Betrieb nehmen dürfen, wenn sie abhörfähig und entsprechend getestet ist, sondern dass sich mit dem Kreis der Mitwirkungspflichtigen auch das *Risiko für illegale Abhörmaßnahmen erweitert*.

Das *Begleitgesetz zum Telekommunikationsgesetz* von 1997 hat diese erweiterten Mitwirkungspflichten auch in die Abhörbestimmungen nach dem G-10 und §§ 100a ff StPO aufgenommen und die Überwachungsmöglichkeiten auf *E-Mail-Adressen, IP-Nummern und Internet-Namen* erstreckt.

Das Bundeswirtschaftsministerium legte 1998 den Entwurf für eine Nachfolgeverordnung für die Fernmeldeüberwachungsverordnung, die sog. *Telekommunikationsüberwachungsverordnung* (TKÜV) vor, der die Einrichtung von permanenten Schnittstellen für die jederzeitige zeitgleiche Überwachung jeder Kommunikationsverbindung vorsah. Zugleich sollte eine Technische Richtlinie "Internet" die Einzelheiten der Internet-Überwachung regeln. Beide Entwürfe wurden nach einhelliger Kritik aus der Wirtschaft und vonseiten der Datenschutzbeauftragten im vergangenen Jahr zurückgezogen. *Neuere Überlegungen* des *Bundeswirtschafts-ministeriums* für eine Telekommunikationsüberwachungsverordnung zeigen zwar, dass der Umfang der Überwachungsverpflichtungen begrenzt werden soll. Mit Hilfe von Ausnahmeregelungen auf der Verordnungsebene ist das Problem der überschießenden gesetzlichen Überwachungsbefugnisse aber nicht zu lösen. Das Telekommunikationsgesetz selbst muss geändert werden.

5. Bundesweiter Zugriff auf Kundendateien

Darüber hinaus verpflichtet das Telekommunikationsgesetz von 1996 alle, die geschäftsmäßig Telekommunikationsdienste anbieten, also nicht nur lizenzpflichtige Telefongesellschaften wie die Telekom und ihre Wettbewerber, sondern nach dem Wortlaut des Gesetzes auch jedes Unternehmen, das Inhouse-Netze und Nebenstellenanlagen z.B. in Krankenhäusern und Hotels betreibt, *"Kundendateien"* zu führen, auf die die Sicherheitsbehörden jederzeit online und unbemerkt über die Regulierungsbehörde zugreifen dürfen. Der Sinn dieser Vorschrift bestand ursprünglich darin, in einem liberalisierten Telekommunikationsmarkt den Sicherheitsbehörden die Feststellung zu ermöglichen, bei welcher Telefongesellschaft eine verdächtige Person Kundin oder Kunde ist, um den zu überwachenden Anschluss identifizieren zu können. Das Gesetz ist aber in diesem Punkt so blankettartig formuliert, dass es auch die Nutzung der bei der Regulierungsbehörde vorliegenden Kundendateien als *bundesweites Adress- und Einwohnerregister* zulässt, ohne dass die so gewonnenen Informationen zur Überwachung des Telekommunikationsverkehrs genutzt werden müssen. Noch 1990 hatte der Einigungsvertrag aus guten Gründen - nicht nur wegen der Querverbindung zur Staatssicherheit - die Auflösung des Zentralen Einwohnerregisters der ehem. DDR vorgeschrieben. Ungeklärt ist im Übrigen, wie die Kundendateien gegen Hackerangriffe wirksam geschützt werden können.

6. Überwachungsvorschrift aus der analogen Telefonwelt wieder belebt

Hinzu kommt, dass der aus der Zeit des analogen Telefonverkehrs stammende *§ 12 Fernmeldeanlagengesetz* nach wie vor in Kraft ist. Er erlaubt den Sicherheitsbehörden unter relativ einfachen Voraussetzungen den Zugriff auf

Daten über die Telekommunikation, obwohl seit der Digitalisierung der Telekommunikation ein wesentlich umfangreicherer und aussagekräftigerer Datenkranz bei den Unternehmen, die Telekommunikation anbieten, gespeichert wird. Er entspricht nicht den Voraussetzungen, die das Bundesverfassungsgericht für Einschränkungen des Fernmeldegeheimnisses verlangt. Obwohl eine Einschränkung von § 12 FAG bei der Verabschiedung des TKG in Aussicht gestellt wurde, steht zu befürchten, dass seine Weitergeltung nach Ablauf der Frist Ende 1999 beschlossen wird.

7. Europäische Überwachungsstruktur im Aufbau (ENFOPOL)

Auch auf europäischer Ebene wird an einer *Intensivierung der Kommunikationsüberwachung* gearbeitet. Die Ratsarbeitsgruppe "Polizeiliche Zusammenarbeit" hat unter der Bezeichnung *"ENFOPOL 98"* Vorschläge für eine Entscheidung des Rates zur "Überwachung des Telekommunikationsverkehrs in Bezug auf neue Technologien" erarbeitet, die lange Zeit der Öffentlichkeit vorenthalten wurden. Hauptziel dieser Vorschläge ist es vordergründig, die Überwachungsmöglichkeiten der Polizei den neuen Technologien wie z.B. der Satellitentelefonie anzupassen. Zugleich sollen aber technische Überwachungsmöglichkeiten auf europäischer Ebene verabredet werden, für deren Ausnutzung zumindest in der Bundesrepublik die materielle Rechtsgrundlage fehlt. So verlangen die Sicherheitsbehörden in der Bundesrepublik bei Mobilfunkgesellschaften den Zugriff auf Personalien solcher Kundinnen und Kunden, die mit den immer populäreren datenschutzfreundlichen Guthabenkarten telefonieren wollen. Diese Forderung der Sicherheitsbehörden ist ebenso wenig nach dem Telekommunikationsgesetz gerechtfertigt wie es die Forderung nach einer Identifizierung all der Personen wäre, die bei der Telekom Telefonkarten für das Festnetz kaufen. Auch wenn der Europäische Rat die Entscheidung über diese Vorschläge im Mai 1999 noch vertagt hat, besteht zwischen den Regierungsvertretern in der Sache offenbar bereits Einigkeit.

Sowohl national wie auf europäischer Ebene tragen technische Überwachungsvorschriften auch dann zum *Aufbau einer Überwachungsmentalität* bei, wenn sie nur unter den materiellen gesetzlichen Voraussetzungen z.B. nach der Strafprozessordnung genutzt werden dürfen. Weil eine Überwachung der Telekommunikation technisch immer einfacher und umfassender möglich ist, sinkt das Rechtsbewusstsein für die Schwere des Rechtseingriffs. Dies lässt - weil technisch leicht umsetzbar - den Eingriff in das Fernmeldegeheimnis auch völlig Unverdächtiger als weniger gravierend erscheinen. Außerdem droht eine Absenkung des Schutzes der vertraulichen Telekommunikation über europäisch harmonisierte Überwachungsstandards, weil in sie auch die Rechtsvorstellungen von Ländern in Europa eingehen, in denen das Fernmeldegeheimnis keinen vergleichbar hohen Stellenwert hat wie in der Bundesrepublik.

8. Erweiterte Rolle der "Dienste"

Zusätzlich ist zu berücksichtigen, dass der Telekommunikationsverkehr offenbar auch von in- und ausländischen *Geheimdiensten* überwacht wird. Dabei spielt neben dem klassischen Aufgabenfeld dieser Dienste die *Wirtschaftsspionage* eine immer größere Rolle. Gleichzeitig ist eine *Aufweichung des* traditionell in der Bundesrepublik geltenden und von den Alliierten vor dem Hintergrund historischer Erfahrungen eingeführten *Trennungsgebots* zu beobachten. Danach sind Aufgaben und Mittel der Strafverfolgungs- und Polizeibehörden von den Aufgaben und Methoden der Geheimdienste im Interesse einer rechtsstaatlichen Kontrolle strikt zu trennen. Gerade im Bereich der Telekommunikationsüberwachung dürfen Polizei und Staatsanwaltschaft nicht zum verlängerten Arm des Verfassungsschutzes oder anderer "Dienste" werden. Umgekehrt hat das Bundesverfassungsgericht den Informationsfluss vom Bundesnachrichtendienst zu den Strafverfolgungsbehörden bei der verdachtslosen Rasterfahndung in der grenzüberschreitenden Telekommunikation an enge Voraussetzungen geknüpft und dem Gesetzgeber aufgegeben, einen verfassungskonformen Zustand herzustellen.

III. Forderungen

Vor diesem Hintergrund fordern die *Datenschutzbeauftragten Berlins, Bremens, Nordrhein-Westfalens, Schleswig-Holsteins sowie der Datenschutz- und Informationszugangsbeauftragte Brandenburgs* eine grundlegende Änderung der deutschen Kommunikationspolitik. Nicht der unbedingte Wille, nirgendwo "abhörfreie Zonen" entstehen zu lassen, sondern der aktive Schutz des Grundrechts der Bürgerinnen und Bürger auf freie und unbeobachtete Telekommunikation müssen im Vordergrund stehen. Deutschlands Weg in die Informations- und Kommunikationsgesellschaft ist rechtsstaatlich und demokratisch nur zu verantworten, wenn er mit klaren Garantien für die Grundrechte verbunden ist.

Der Bundesgesetzgeber muss über die vom Bundesverfassungsgericht angeordnete Modifikation des G-10-Gesetzes hinaus ein *Gesetz zur Sicherung der freien Telekommunikation* verabschieden. Grundlage muss eine *Evaluierung* der bisherigen Eingriffe in das Telekommunikationsgeheimnis sein. Mit ihrer Hilfe sind die bestehenden, in den vergangenen Jahren ständig erweiterten Überwachungsbefugnisse der Strafprozessordnung, des G-10 sowie des Außenwirtschaftsgesetzes auf ihre Notwendigkeit nach objektiven Kriterien zu prüfen.

Folgende Maßnahmen sind unverzichtbar:

1. Verpflichtung zur Datensparsamkeit und Datenvermeidung

Je weniger Daten personenbezogen verarbeitet werden, desto geringer sind die Eingriffsmöglichkeiten. Wer Angebote zur Telekommunikation macht, sollte ausserdem verpflichtet werden, den Kundinnen und Kunden eine Option zur anonymen Nutzung des Telekommunikationsnetzes (z. B. durch Einsatz von Guthabenkarten auch bei häuslichen Festnetzanschlüssen) zur Verfügung zu stellen. Hilfreich könnte hierfür die Einführung der Möglichkeit sein, förmliche Audits zur Bewertung besonders datenschutzfreundlicher Telekommunikationsdienste durchzuführen.

2. Verschlüsselung als Standardleistung anbieten

Wer Telekommunikation anbietet, sollte verpflichtet werden, kostenlos Verschlüsselungsmöglichkeiten als Universaldienstleistung anzubieten, ohne dass damit die generelle Verpflichtung zur Bereitstellung von Abhörschnittstellen für die Polizei und die Geheimdienste verbunden ist.

3. "Mediennutzungsgeheimnis" einführen

In das Teledienstedatenschutzgesetz des Bundes (und entsprechend auch in den Mediendienstestaatsvertrag der Länder) sollte ein ausdrückliches Mediennutzungsgeheimnis aufgenommen werden, um die verfassungsrechtliche Ausstrahlungswirkung des Kommunikationsgeheimnisses nach Artikel 10 GG auf einfachgesetzlicher Ebene klarzustellen. Ebenso wenig wie Zeitungsleserinnen und -leser es hinnehmen müssen, dass registriert wird, welche Zeitung sie in Papierform täglich lesen, ist eine Überwachung ihrer Medienpräferenz akzeptabel, wenn sie die Zeitung im Internet (als "webzine") liest.

4. Mitwirkungspflichten bei Abhörmaßnahmen begrenzen

Die Pflicht zur Durchführung von staatlichen Überwachungsmaßnahmen muss durch Änderung des Telekommunikationsgesetzes und der entsprechenden Begleitgesetze auf diejenigen begrenzt werden, die öffentliche, lizenzpflichtige Telekommunikationsdienste erbringen. Nebenstellenanlagen in Hotels, Betrieben und Krankenhäusern usw. wären dann ausgenommen.

5. Überwachungsbefugnisse evaluieren

Überwachungsmassmahmen bei der Telekommunikation müssen erstmals einer echten Effektivitätskontrolle unterzogen werden, auf deren Grundlage der Gesetzgeber ständig die Notwendigkeit der Beibehaltung bestimmter Befugnisse zu Eingriffen in das Kommunikationsgeheimnis in bestimmten Zeitabständen überprüfen sollte. Die gegenwärtig vorgeschriebene Geheimhaltung der entsprechenden Statistiken (§ 88 Abs.5 Satz 3 TKG) ist nicht länger zu rechtfertigen.

6. Datenschutzfreundliche Techniken fördern

Die Bundesregierung wird aufgefordert, die Bürgerinnen und Bürger beim Schutz ihres Telekommunikationsgeheimnisses gegen illegales Abhören durch in- oder ausländische private Dritte zu unterstützen. Hierfür kommt in Betracht:

a) Der verstärkte Mitteleinsatz für die Erforschung und Entwicklung datenschutzfreundlicher Telekommunikationstechniken im Netz- und im Endgerätebereich.

b) Die Förderung von Tests auf Praktikabilität und Wirksamkeit entsprechender Techniken und ihrer kundenfreundlichen Markteinführung.

7. Berufliche Schweigepflichten wirksam schützen

Die Bundesregierung wird aufgefordert, eine geschlossene Konzeption für den besonderen Schutz der Telekommunikation von *Berufsgruppen*, die *besonderen Verschwiegenheitspflichten* unterliegen wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen usw. vorzulegen.

8. Strafrechtlichen Schutz des Kommunikationsgeheimnisses endlich ernst nehmen

Die Bagatellisierung von *Straftaten gegen den Schutz der Privatsphäre* ist zu beenden, z. B. durch:

a) stärkere polizeiliche Prävention gegen illegales Abhören

b) die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik

c) eine Effektivierung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen

d) die Prüfung, ob nicht ähnlich wie in anderen Bereichen Hackerangriffe straffrei bleiben sollten, wenn dabei festgestellte Sicherheitslücken in Telekommunikationsnetzen sofort angezeigt werden.

C. Beschlüsse der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation

Gemeinsamer Standpunkt zu Datenschutz bei Gebäude-Bilddatenbanken

angenommen auf der 25. Sitzung der Arbeitsgruppe am 29. April 1999 in Norwegen

- Übersetzung -

Computer haben die Fähigkeit, Informationen aus einer Reihe von Quellen einschließlich öffentlicher Register zu verknüpfen und zugänglich zu machen. Im Zusammenhang mit der Entwicklung von Geographischen Informationssystemen (GIS), die die Ortsbestimmung ermöglichen, und digitaler Fotografie- bzw. Bilderstellung kann dies das leichte Auffinden großer Informationsmengen durch Verknüpfung mit Adressen oder Planangaben (-koordinaten) ermöglichen. Darin liegt eine wachsende Bedrohung für die Privatsphäre einzelner Bürger. Eine aktuelle Entwicklung ist die systematische Sammlung digitaler Bilder von Gebäuden zum Aufbau von Gebäude-Bilddatenbanken ganzer Städte für kommerzielle Zwecke. Während es wichtige und legitime Anwendungen für Geographische Informationssysteme und digitale Aufnahmen von Gebäuden gibt, z. B. für Planungszwecke, muss die Position der Betroffenen hinsichtlich der kommerziellen Nutzung dieser Datenbanken gestärkt werden.

So setzen gegenwärtig beispielsweise Unternehmen in mehreren Ländern mobile Digitalkameras ein, die auf Kleintransportern montiert sind, um Bilder aller Gebäude in größeren Städten aufzuzeichnen. Die Daten können dann auf CD-ROM gespeichert und der Feuerwehr, der Polizei und Notfalldiensten zur Vorbereitung ihrer Einsätze angeboten werden. Es liegt aber auf der Hand, dass eine solche Datenbank auch für kommerzielle Zwecke genutzt werden kann. Die Bilder können mit Hausnummern, Namen und Adressen von Eigentümern und Bewohnern zur Beurteilung der Bonität (Scoring) oder Risiken durch Banken und Versicherungen auf Grund des Gebäudezustandes oder einer Einstufung der Wohngegend bzw. für Zwecke der Direktwerbung verknüpft werden. Die Daten können für fernsehgestützte Bilddatenbanken oder für Planungszwecke von Transportunternehmen (Lieferfirmen,Taxis usw.) verwendet werden. Sie werden oft mit Daten verknüpft, die mit Hilfe von Satelitten erhoben werden (Global Positioning System - GPS), und können dann genutzt werden, um realistische digitale Stadtpläne zu erzeugen und eine neue Generation Geographischer Informationssysteme zu unterstützen. Obwohl gegenwärtig - abhängig vom eingesetzten System - Probleme der Speicherkapazität und Verarbeitungsgeschwindigkeit auftreten können, wird sich dies wahrscheinlich ändern.

Es muss deutlich gemacht werden, dass eine totale Registrierung aller Gebäude in einer Stadt oder in einem Land zu einer Verarbeitung personenbezogener Daten führen wird, da ein Großteil der Informationen sich auf natürliche Personen bezieht, die durch Zuordnung zu spezifischen Elementen als Ausdruck ihrer physischen, wirtschaftlichen, kulturellen oder sozialen Identität bestimmbar sind (vgl. Artikel 2 a) und c) der Richtlinie 95/46/EG) und die direkt oder indirekt mit Verzeichnissen verknüpft werden können. Deshalb unterliegt die Schaffung von Bilddatenbanken dieser Art den nationalen Datenschutzgesetzen in Über- einstimmung mit der EG-Datenschutzrichtlinie. Wo dies nicht bereits der Fall ist, sollte die nationale Gesetzgebung dem Betroffenen zumindest ein Widerspruchsrecht gegen die systematische Sammlung und Speicherung derartiger Bilddaten über seine Wohnumgebung für kommerzielle Zwecke einräumen. Die Tatsache, dass diese Informationen bereits zu einem gewissen Grad öffentlich zugänglich sind, schließt sie nicht von der Anwendung der Datenschutzgesetze aus. Darüber hinaus kann die Veröffentlichung solcher Datenbanken Sicherheitsprobleme für die Betroffenen (Eigentümer, Mieter oder Bewohner) verursachen. Es gibt 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.

Gemeinsamer Standpunkt zu intelligenten Software-Agenten

angenommen auf der 25. Sitzung der Arbeitsgruppe am 29. April 1999 in Norwegen

- Übersetzung -

Ein Software-Agent wird definiert als ein Software-Produkt, das anstelle seines Benutzers agiert und versucht, ohne einen direkten Eingriff oder eine direkte Überwachung des Benutzers bestimmte Objekte zu finden oder bestimmte Aufgaben zu erledigen. Agenten können in verschiedener Weise bei der Telekommunikation verwendet werden. An erster Stelle können sie dazu benutzt werden, die Funktionalität eines Telekommunikationsnetzes zu erweitern. Es ist möglich, ein Netzwerk effizienter zu benutzen, wenn die Ressourcen an die Anforderungen der einzelnen Nutzer angepasst sind. Agenten können diese Aufgabe übernehmen, in dem sie die Nutzer repräsentieren.

Eine andere Anwendung bezieht sich auf inhaltliche Mehrwertdienste, die mit Mitteln der Telekommunikation verbreitet werden: Agenten können im Auftrag des Nutzers verwendet werden, um Informationen (z.B. im Internet) zu selektieren und zu sammeln, sowie als Mittler gegenüber anderen Teilnehmern bei elektronischen Transaktionen auftreten. Im Augenblick stehen die ersten Dienste dieser Art zur Verfügung, ausgehend von einer einfachen

„Push-Technologie“, die Informationen auf der Basis individuell spezifizierter Interessen dem Benutzer ins Haus bringt, bis hin zu komplizierten Systemen, die es gestatten, die Nutzung des Netzes zu personalisieren und die Aktivitäten der Nutzer nachzuvollziehen.

Die Entwicklung der Agenten-Technologie wird in intelligenten Software-Agenten gipfeln, Software-Programmen, mitunter mit dedizierter Hardware gekoppelt, die dazu bestimmt ist, komplette Aufgaben im Auftrag der Nutzer zu erledigen. In ihrer Rolle als Repräsentant einer Person wird eine Vielzahl personenbezogener Informationen erzeugt und durch die Operationen der Agenten verbreitet werden. Der Schutz der Privatsphäre und die Vertraulichkeit der Netzaktivitäten werden eines der größten Probleme sein, mit denen die Nutzung intelligenter Agenten in der Zukunft konfrontiert sein wird.

Dieser gemeinsame Standpunkt zielt darauf ab, eine erhöhte Aufmerksamkeit für die Risiken für die Privatsphäre zu erzeugen, die mit der Nutzung von Agenten verbunden sind, und die Systemdesigner zu ermutigen, Maßnahmen zum Schutz der Privatsphäre einzubauen. Die Risiken für die Persönlichkeitsrechte, die mit der Nutzung von Agenten verbunden sind, können wie folgt zusammengefasst werden:

Erstens: Risiken, die mit der Tatsache zusammenhängen, dass ein Agent im Auftrag eines Nutzers handelt. Nutzerprofile stellen einen wesentlichen Anteil der Aktivitäten von Agenten dar. Typischerweise umfasst das Nutzerprofil Informationen über Identität und Kommunikationspartner sowie eine Vielzahl von Informationen über persönliche Präferenzen. Wenn ein Agent im Netz operiert, werden personenbezogene Daten mit der Umgebung ausgetauscht und möglicherweise an nicht autorisierte dritte Parteien weitergegeben.

Zweitens: Risiken, die mit fremden Agenten verbunden sind, die im Auftrag anderer Teilnehmer handeln. Agenten oder allgemeiner ihre Nutzer, könnten mit Agenten konfrontiert werden, die im Auftrag anderer Teilnehmer handeln. Diese könnten freiwillig personenbezogene Daten von Individuen sammeln, indem sie eine Verkehrsanalyse durchführen, in Datenbanken eindringen, die Informationen über die Individuen enthalten, oder das Nutzerprofil eines Agenten zugänglich machen. Derartige Agenten können sogar verkleidet auftreten oder andere Agenten ausschalten.

Empfehlungen:

Maßnahmen müssen ergriffen werden, um das Auftreten von Risiken für die Privatsphäre durch intelligenten Software-Agenten zu reduzieren. Die Arbeitsgruppe empfiehlt, dass Folgendes Berücksichtigung findet, wobei die

Anforderungen, die die Datenschutzprinzipien stellen, insbesondere diejenigen, die sich aus dem Zweck ergeben, für den der Agent erstellt worden ist, berücksichtigt werden müssen:

1. Software-Hersteller sollten in einem frühen Designstadium die Auswirkungen der Nutzung intelligenter Agenten für die Privatsphäre des Einzelnen bedenken. Dies ist notwendig, um die Konsequenzen, die in naher Zukunft entstehen könnten, unter Kontrolle zu halten.

2. Entwickler von Agenten sollten sicherstellen, dass die Nutzer die Kontrolle über ihre Systeme und die darin enthaltenen Informationen nicht verlieren. Sie sollten dem Nutzer ein Maximum an Transparenz über die Funktionsweise des Agenten verschaffen. Wenn Kontroll- und Feedbackmechanismen sowie Sicherheitsvorkehrungen hinzukommen, wird dies den Nutzern von Agenten helfen, Vertrauen bei der Nutzung der Agententechnologie zu verbessern.

3. Entwickler von intelligenten Agenten sollten geeignete Mittel zur Verfügung stellen, durch die die Privatsphäre der Nutzer geschützt und die Kontrolle der Betroffenen über die Nutzung ihrer personenbezogenen Daten aufrechterhalten werden kann.

4. Technische Maßnahmen sowie Privacy Enhancing Technologies (PET) werden in Verbindung mit den Software-Agenten empfohlen. Die folgenden Maßnahmen werden vorgeschlagen:

   - Entwicklung einer Trusted-Third-Party-Struktur für die Verifizierung und Authentifizierung aller Agenten
   - Zugangskontrollmechanismen

   - Werkzeuge, die dem Nutzer die Kontrolle über die Aktionen von Agenten Dritter Teilnehmer verschaffen, die personenbezogene Daten sammeln

   - Mechanismen, die aufgezeichneten Aktivitäten nachzuvollziehen

   - Integritätsmechanismen, um die Integrität der gespeicherten oder ausgetauschten Daten sicherzustellen und die Integrität der Arbeitsmethoden der Agenten oder der zertifizierten Komponenten wie digitale Signaturen zu kontrollieren.

Diese Maßnahmen müssen in die Agenten integriert werden. Die Maßnahmen können auch genutzt werden, um eine Infrastruktur vertrauenswürdiger Komponenten aufzubauen.

5. Anhand einer Checkliste für datenschutzfreundliche Designkriterien sollten die Entwickler, Lieferanten oder Provider eines Agenten den Agenten oder die Umgebung des Agenten mit geeigneten Privacy Enhancing Technologies ausrüsten. Rahmenbedingungen für die Zertifizierung der Datenschutzfreundlichkeit von Software-Agenten sind notwendig.

Gemeinsamer Standpunkt zur Sprechererkennung und Stimmerkennungstechnologien in der Telekommunikation

angenommen auf der 25. Sitzung der Arbeitsgruppe am 29. April 1999 in Norwegen

- Übersetzung -

Unter den gegenwärtig entwickelten biometrischen Identifikationsmethoden ist die Sprechererkennung wahrscheinlich die fortschrittlichste und von besonderer Relevanz für die Telekommunikation.

Sprechererkennung ist eine Methode, die Eigenschaften der Stimme einer Person zu analysieren, um

- die Stimme eines unbekannten Sprechers zu identifizieren;

- zu verifizieren, dass ein Sprecher derjenige ist, der er behauptet zu sein (Authentifikation);

- die Stimme einer Person in einer Umgebung mit vielen Sprechern zu erkennen.

In allen Fällen wird die Stimme einer Person gemessen und mit einem zuvor aufgenommenen und gespeicherten Muster oder Stimmabdruck der Stimme verglichen.

Die besten Ergebnisse beim Erkennen der Personen werden in Bezug auf die Fehlerraten erzielt, wenn die gleichen Wörter für die Eingabe und das Muster verwendet werden (text dependent systems). Zu denken ist an ein vorher festgelegtes Passwort oder eine Identifikationsnummer. Nach der Eingabe wird dieses mit dem gespeicherten Stimmabdruck verglichen.

In anderen Systemen werden die Sprecher veranlasst, zufällig ausgewählte Wörter zu wiederholen, die mit dem Muster verglichen werden (text prompted systems). Der Vorteil ist hier, dass das System nicht fehlgeleitet werden kann durch Fälscher, die auf Band gespeicherte Stimmabdrücke missbrauchen.

In "text independent systems" wird eine Person gebeten zu sprechen, und ihre Äußerungen werden mit den gespeicherten Mustern verglichen, die völlig verschiedene Wörter enthalten. Dies beinhaltet einen erheblich höheren Zufallsfaktor, und von daher ist der Vergleich schwieriger, besonders wenn Hintergrundgeräusche vorliegen oder Telefonleitungen mit hohem Geräuschpegel verwendet werden. Auf der anderen Seite ist das Potential hoch: In Verbindung mit einer großen Sammlung von Stimmmustern ermöglichen textunabhängige Systeme die Identifizierung vieler verschiedener Personen in verschiedenen Umgebungen.

Die Sprechererkennung kann genutzt werden für die Identifikation und Authentifikation sowohl für den Zugang zu Netzen und Anlagen als auch für den Zugang zu Diensten, die über das Netz verbreitet werden. Offensichtlich haben Telekombetreiber ein Interesse an verbesserter Stimmidentifizierung und Authentifizierung zu verschiedenen Zwecken, z. B. Abrechnungsbetrug zu bekämpfen oder neue Funktionen und Dienste zu vermarkten. Was Dienste betrifft, die über Telekommunikationsdienste verbreitet werden, wird die Identifikation von Kunden zunehmend als wesentlich für Online-Entscheidungen betrachtet, bei denen ein Individuum beteiligt ist. Es muss bemerkt werden, dass anders als die meisten anderen biometrischen Identifikationsmethoden die Sprechererkennung keine neue Infrastruktur erfordert, sie kann vielmehr in die bestehenden Telekommunikationsnetze integriert werden.

Die Nutzung der Sprechererkennung ist noch beschränkt auf bestimmte Anwendungen. Die Kosten dieser Technologie werden erwartungsgemäß allerdings schnell sinken, während die Qualität der Systeme wächst. In naher Zukunft können Massenanwendungen erwartet werden.

Die Datenschutzbeauftragten haben bei anderer Gelegenheit festgestellt, dass anonyme Methoden für den Zugang zu Telekommunikationsnetzen und anonyme Zahlungsmethoden zwei wesentliche Elemente echter Online-Anonymität sind.

Die Internationale Arbeitsgruppe ist besorgt über das Risiko, dass diese Techniken in der Telekommunikation eingesetzt und genutzt werden können, ohne Kenntnis der Nutzer und ohne Mittel, sie zu umgehen.

Empfehlungen

1. Die Einführung und Nutzung von Sprechererkennungstechnologien in Telekommunikationsnetzen sollte auf Umstände beschränkt werden, bei denen die Authentifikation wesentlich ist.

2. Da diese Identifikationsmethode unvermeidlich eine bestimmte Fehlerquote hat, sollte sie nicht eingeführt werden, ohne dass Schadensersatzansprüche zur Verfügung stehen.

3. Die informierte Einwilligung der Betroffenen sollte eingeholt werden, bevor Sprachanalysetechnologien angewandt werden. Grundsätzlich sollte diese Technologie auch mit deren Einwilligung nicht angewandt werden, um den geistigen oder emotionalen Zustand einer Person zu ermitteln.

4. Den Betroffenen sollte die Möglichkeit gegeben werden, anonym zu bleiben, wo dies angemessen ist.

5. Provider sollten die Betroffenen informieren, wenn ihre Stimmmuster in einer Datenbank gespeichert werden. Diese Information sollte auch klarstellen, unter welchen Umständen die Daten genutzt werden sollen.

6. Anbieter, in deren Auftrag eine Identifikation anhand einer Sprechererkennung stattfindet, sollten den Betroffenen über ihre Identität und den Zweck informieren, für den die Identifikation erforderlich ist.

D. Arbeitspapier der Datenschutzbeauftragten der Europäischen Union (Gruppe nach Art. 29 der Datenschutzrichtlinie der EU)

Empfehlung 1/99

Über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware

Von der Arbeitsgruppe am 23. Februar 1999 angenommen

(WP 17 - 5093/98 - DE endgültig)

DIE GRUPPE FÜR DEN SCHUTZ DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.Oktober 1995,

gestützt auf Artikel 29 und 30 Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14 Absatz 3,

EMPFIEHLT:

1. Die Gruppe fordert die Software- und Hardwareindustrie auf, Internetprodukte zu erarbeiten, die den Schutz der Privatsphäre gewährleisten und die zur Einhaltung der europäi- schen Datenschutzvorschriften notwendigen Mittel beinhalten.

   Eine Voraussetzung für die rechtmäßige Verarbeitung personenbezogener Daten ist die Unterrichtung des Betroffenen, damit er von der jeweiligen Verarbeitung Kenntnis hat. Daher ist die Gruppe insbesondere über alle Arten von Verarbeitungsvorgängen besorgt, die gegenwärtig über Software und Hardware im Internet ablaufen, ohne dass die Betroffenen hiervon Kenntnis haben, die für sie also "unsichtbar" sind.

Typische Beispiele für eine solche unsichtbare Verarbeitung sind das "Chattering" auf HTTP-Ebene, automatische Hyperlinks zu Dritten, aktive Inhalte (wie Java, ActiveX oder andere nutzerorientierte Scripttechniken) sowie die Cookie-Merkmale, die zurzeit in den üblichen Browsern vorhanden sind.

2. Alle Internet-Software- und Hardwareprodukte sollten den Internetbenutzer darüber informieren, welche Daten sie sammeln, speichern und übertragen wollen und aus welchem Grund sie erforderlich sind.

   Ferner sollten Internet-Software- und Hardwareprodukte dem Datenbenutzer ermöglichen, später jederzeit problemlos Zugang zu den über ihn gesammelten Daten zu erhalten.

   Dies bedeutet beispielsweise:

   - bei einer Browser-Software, dass sie bei der Herstellung der Verbindung mit einem Webserver (Senden einer Anfrage oder Erhalt einer Webseite) den Benutzer darüber aufklärt, welche Informationen zu welchem Zweck übertragen werden soll;

   - bei von einer Webseite an den Benutzer gesendeten Hyperlinks, dass der Browser des Benutzers ihm diese - unabhängig von der Methode - alle anzeigt;

   - bei Cookies, dass der Benutzer darüber unterrichtet wird, wenn die Internetsoftware ein Cookie empfangen, speichern oder senden will. Diese Mitteilung sollte in allgemein verständlicher Sprache erklären, welche Information zu welchem Zweck in diesem Cookie gespeichert werden soll und wie lange das Cookie gilt.

3. Die Konfiguration von Hardware- und Software-Produkten sollte keine Standardeinstellung beinhalten, die das Sammeln, Speichern oder Versenden der im Client vorgehaltenen Daten zulässt. Zum Beispiel:

   - Die Browsersoftware sollte standardmäßig so konfiguriert sein, dass nur die unbedingt zur Herstellung der Internetverbindung erforderlichen Informationen verarbeitet werden. Cookies sollten nie standardmäßig gespeichert oder gesendet werden.

- Bei der Installation eines Browsers sollte dessen Funktion für die Speicherung und den Versand der Daten über die Identität oder das Kommunikationsverhalten des Benutzers (Profil) nicht automatisch mit derartigen, zuvor schon im Rechner des Benutzers abgespeicherten Daten versorgt werden.

4. Internet-Hardware- und Softwareprodukte müssen dem Betroffenen die freie Entscheidung über die Verarbeitung seiner personenbezogenen Daten ermöglichen und zwar mit benutzerfreundlichen Tools zur Selektion (d.h. Ablehnung oder Änderung) für den Empfang, die Speicherung bzw. den Versand client-persistenter Informationen anhand bestimmter Kriterien (u.a. Profile, Bereich oder Identität des Internetservers, Art und Dauer der gesammelten, gespeicherten bzw. versandten Informationen usw.). Der Benutzer sollte klare Anweisungen über die Verwendung von Soft- und Hardware zur Implementierung dieser Optionen und Tools erhalten. Zum Beispiel:

5. Die Browser-Software sollte dem Benutzer Konfigurationsoptionen bieten, damit er vorgeben kann, welche Daten sie sammeln und übertragen soll oder nicht.

6. Im Falle der Cookies bedeutet dies, dass der Benutzer immer die Option haben muss, das Senden oder Speichern eines Cookies insgesamt zuzulassen oder abzulehnen. Ferner sollte er entscheiden können, welche Informationsbestandteile eines Cookies beibehalten oder entfernt werden sollen, z.B. je nach der Gültigkeitsdauer des Cookies oder der sendenden oder empfangenden Webseiten.

7. Internet-Software- und Hardwareprodukte sollten es den Benutzern ermöglichen, client-persistente Informationen einfach und ohne Beteiligung des Senders zu entfernen. Der Benutzer sollte klare Anweisungen darüber erhalten, wie dies zu tun ist. Falls die Information nicht entfernt werden kann, muss zuverlässig sichergestellt werden, dass sie nicht übertragen und gelesen wird.

- Cookies und andere client-persistente Informationen sollten entsprechend eines bestimmten Standards im Client-Computer gespeichert werden und leicht und selektiv zu löschen sein.

HINTERGRUND

Momentan ist es unmöglich, das Internet zu verwenden, ohne ständig auf Funktionalitäten zu stoßen, die die Privatsphäre verletzen und, für den Betroffenen unsichtbar, alle möglichen Verarbeitungsprozesse personenbezogener Daten vornehmen. Mit anderen Worten, der Internet-Benutzer weiß nichts davon, dass seine personenbezogenen Daten gesammelt und weiterverarbeitet wurden und für ihm unbekannte Zwecke genutzt werden könnten. Der Betroffene hat keine Kenntnis von dieser Verarbeitung und keine diesbezügliche Entscheidungsfreiheit.

Ein Beispiel für diese Technik ist das so genannte Cookie, das man definieren könnte als einen Computer-Informationseintrag, der von einem Webserver an den Computer des Benutzers gesandt wird, um ihn bei späteren Besuchen auf der gleichen Webseite wieder identifizieren zu können.

Browser sind Softwareprogramme, die u.a. dafür geschrieben wurden, das im Internet vorhandene Material graphisch anzuzeigen. Ein Browser kommuniziert zwischen dem Computer des Benutzers (Client) und dem entfernten Computer, auf dem die Informationen gespeichert sind (Webserver). Häufig senden die Browser mehr Informationen an den Webserver als zur Herstellung der Kommunikation eigentlich erforderlich ist. Die klassischen Browser teilen dem angewählten Webserver automatisch die Art und Sprache des anwählenden Browsers mit, die Bezeichnungen weiterer auf dem Benutzer-PC installierter Softwareprogramme und Betriebssysteme, die Seite, von der der Verweis kommt, Cookies usw. Solche Daten können von der Browser-Software auch unbemerkt systematisch an Dritte übertragen werden.

Mit diesen Techniken lassen sich so genannte Clicktrails über den Internet-Benutzer anlegen. Clicktrails beinhalten Informationen über das Verhalten einer Person, deren Identität, Suchweg oder Auswahlverhalten beim Besuch der Webseite. Sie enthalten die Links, die der Benutzer aufgerufen hat und die auf dem Webserver protokolliert sind.

Die europäischen Datenschutz-Richtlinien 95/46/EG und 97/66/EG enthalten detaillierte Be- stimmungen für den Schutz der Rechte von Personen hinsichtlich ihrer personenbezogenen Daten. Beide Richtlinien sind für die in dieser Empfehlung behandelten Belange von Bedeutung, da es hier um die Verarbeitung der personenbezogenen Daten der Internet-Benutzer geht. Cookies oder Browser können Daten enthalten oder weiter verarbeiten, die eine direkte oder indirekte Identifizierung des einzelnen Internet-Benutzers ermöglichen.

Die Anwendung der Bestimmungen über faire Verarbeitung, rechtmäßige Gründe für die Verarbeitung und das Recht des Betroffenen, über die Verarbeitung seiner eigenen Daten zu bestimmen, führten zur vorstehenden Empfehlung.

Besondere Sorge bereiten der Gruppe die Risiken, die die Verarbeitung personenbezogener Daten von Personen in sich birgt, die hiervon keinerlei Kenntnis haben. Die Software- und Hardwareentwickler sind daher aufgerufen, die Grundsätze dieser Richtlinien zu berücksichtigen und zu respektieren, um die Privatsphäre der Internet-Benutzer angemessen zu schützen.

Brüssel, 23. Februar 1999

Für die Gruppe

Der Vorsitzende

Peter HUSTINX