Abgeordnetenhaus BERLIN

Drucksache 16/0772
13.08.2007

16. Wahlperiode

Vorlage – zur Kenntnisnahme –

Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2006

Der Senat von Berlin
SenInnSport – I E AGK 1

An das
Abgeordnetenhaus von Berlin

über Senatskanzlei G Sen

V o r l a g e
- zur Kenntnisnahme -

über Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2006

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Nach § 29 Abs. 2 Berliner Datenschutzgesetz sowie § 18 Abs. 3 Berliner Informationsfreiheitsgesetz erstattet der Beauftragte für Datenschutz und Informationsfreiheit dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit. Der Senat hat dazu nach § 29 Abs. 2 des Berliner Datenschutzgesetzes eine Stellungnahme herbeizuführen und legt diese hiermit dem Abgeordnetenhaus vor.

Berlin, den 26. Juni 2007

Der Senat von Berlin

Klaus Wowereit	Dr. Körting
---	---
Regierender Bürgermeister	Senator für Inneres und Sport

Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2006

(nach § 29 Abs.2 Berliner Datenschutzgesetz)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Einleitung

Leben wir schon in einer *Überwachungsgesellschaft*? Wenn das so ist, welche Aufgabe haben Datenschutzbeauftragte in einer solchen Gesellschaft?

Diese Fragen standen im Vordergrund der 28. Internationalen Konferenz der Datenschutzbeauftragten, zu der der britische Information Commissioner Richard Thomas (der in Großbritannien für den Datenschutz und die Informationsfreiheit zuständig ist) im November 2006 nach London eingeladen hatte. Für Großbritannien kann man heute schon feststellen, dass es sich um eine Überwachungsgesellschaft handelt[1]: Insgesamt rund 4,2 Millionen Videokameras überwachen dort Straßen und Plätze, jeder Einwohner einer britischen Großstadt wird durchschnittlich mindestens 100-mal von einer solchen Kamera erfasst, in London noch erheblich häufiger. In einer nationalen *DNA-Datenbank* sind rund 1,5 Millionen Proben von Personen[2] erfasst, darunter auch Kinder, denen Bagatelldelikte vorgeworfen werden. Der britische Premierminister hat die Bevölkerung aufgefordert, sich freiwillig in dieser Datenbank erfassen zu lassen. Demgegenüber hat der Erfinder der DNA-Identifizierung, Sir Alec Jeffreys, Zweifel geäußert, ob mit einer solchen nationalen Datenbank nicht der Bogen überspannt werde. Das britische Parlament hat die Errichtung einer nationalen Zentraldatei für alle Kinder beschlossen, mit deren Hilfe Kindesmissbrauch bekämpft werden soll. Abgesehen davon, dass dadurch alle britischen Eltern unter Generalverdacht gestellt werden, sollen die Daten von Kindern gutsituierter Eltern (VIPs) einem besseren Datenschutz unterliegen als bei Kindern aus anderen Familien. Diese Liste der Überwachungsmaßnahmen, die auch der Brite George Orwell sich nicht hätte träumen lassen, ist unvollständig.

In Deutschland werden solche Beschreibungen auf britische Zustände gerade von Politikern kopfschüttelnd abgetan mit dem Bemerken, das sei hierzulande unvorstellbar und das wolle auch niemand. Richtig ist sicherlich, dass wir noch keine britischen Zustände haben. Das ist aber kein Grund, sich zufrieden zurückzulehnen und zur Tagesordnung überzugehen. Denn auch in Kontinentaleuropa und gerade in der Bundesrepublik nehmen die Überwachungstendenzen stetig zu. Dabei handeln die Regierenden in bester Absicht, uns vor Gefahren durch *Terrorismus* und andere schwere Straftaten zu schützen. Aber „der Weg zur

Bei jeder Maßnahme, die dem Schutz vor Gefahren durch Terrorismus oder andere schwere Straftaten dienen soll, prüft der Senat kritisch, ob sie einen greifbaren Sicherheitsgewinn haben wird und welche Beeinträchtigungen sich für unbescholtene Bürger ergeben würden. Maßnahmen mit unverhältnismäßigen Auswirkungen auf unbescholtene Bürger unterstützt der Senat weder auf Landesebene noch auf Bundes- oder EU-Ebene.

[1] Lesenswert sind die Zusammenfassung und die öffentliche Diskussionsgrundlage zu dem vom Surveillance Studies Network für die Internationale Datenschutzkonferenz erstellten Bericht zur Überwachungsgesellschaft, abrufbar unter http://www.privacyconference2006.co.uk/files/report_ger.pdf bzw. http://www.privacyconference2006.co.uk/files/discussion_ger.pdf.

[2] Zum Vergleich: Die DNA-Analysedatei des Bundeskriminalamtes enthielt Ende 2006 400.000 Datensätze, wobei täglich 200–300 Datensätze hinzukommen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Unfreiheit ist mit guten Absichten gepflastert[3]“. Wir befinden uns auch in Deutschland auf einer schiefen Ebene, die eher früher als später in eine Überwachungs- und Präventionsgesellschaft führen wird, wenn wir jetzt nicht energisch gegensteuern. Der britische Information Commissioner sprach auf der Londoner Konferenz davon, wir würden in die Überwachungsgesellschaft „schlafwandeln“. Das ist in Deutschland genauso zutreffend wie in Großbritannien.

Die Privatsphäre ähnelt der Luft zum Atmen, die wir zum Überleben brauchen: Wir bemerken erst, wie wichtig sie für uns ist, wenn sie spürbar eingeschränkt wird oder uns ganz abhanden kommt.

Das zurückliegende Jahr hat drastische Einschränkungen des Datenschutzes in Europa und Deutschland bekannt werden lassen, die sich auch in Berlin – vor allem wegen der Vorgaben des Bundesgesetzgebers – ausgewirkt haben oder dies bald tun werden. Auch die Daten von Berliner *Flugpassagieren*, die in die USA reisen oder die USA nur überfliegen wollen, werden generell vorab an die US-amerikanischen Grenzbehörden übermittelt. Dort können sie an andere Sicherheitsbehörden weitergegeben werden und dienen neuerdings dazu, automatisiert die Gefährlichkeit jedes einzelnen Fluggasts in einer Art *Scoring-Verfahren* mithilfe des *Automated Targeting Systems* (ATS) zu berechnen[4]. Auch Berliner Bankkunden wissen aus Presseberichten erst seit dem vergangenen Jahr, dass die Daten ihrer Überweisungen und sonstigen Finanztransaktionen selbst dann in den USA verarbeitet und möglicherweise – wie es heißt, zum Zweck der *Terrorismusbekämpfung* - an das US-Schatzministerium herausgegeben werden, wenn diese Transaktionen keinerlei Bezug zu den USA haben[5]. Das verantwortliche belgische Unternehmen *SWIFT* entzieht sich in diesem Punkt bisher einer unabhängigen Datenschutzkontrolle. Die Glaubwürdigkeit des internationalen Finanzsystems hat durch dieses Vorgehen von SWIFT erheblichen Schaden genommen, sodass die Kreditinstitute auch in Deutschland und Berlin jetzt über datenschutzgerechte Alternativen bei der Abwicklung des Zahlungsverkehrs nachdenken müssen, wenn SWIFT nicht dazu veranlasst werden kann, seine Praxis zu ändern.

Die im April 2006 verabschiedete Europäische Richtlinie zur *Vorratsdatenspeicherung* wird – sollte sie in dieser Form in deutsches Recht umgesetzt werden – zu einem Dammbruch zulasten des Datenschutzes auch in Berlin führen, weil dann jeder Telefonkontakt und jeder Mausklick personenbezogen registriert wer-

[3] so die treffende Überschrift des Kommentars von Richard Herzinger in der WELT v. 14. Januar 2007

[4] dazu näher unter 8.1

[5] dazu näher unter 8.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

den[6]. Eine unbeobachtete und damit freie Kommunikation, wie sie das Grundgesetz für den Regelfall garantiert, wird dann nicht mehr möglich sein. Dies betrifft auch Abgeordnete, Ärzte, Anwälte und Journalisten. Ein nennenswerter Sicherheitsgewinn ist durch diese völlig unverhältnismäßige Pflicht zur lückenlosen Beobachtung aller Nutzer von Kommunikationsnetzen nicht zu erwarten. Stattdessen wird im Gegenteil die Unsicherheit zunehmen, wenn deutlich wird, dass sich auch auf diesem Wege die „Allmachtsphantasien mancher Politiker von einer kriminalitätsfreien Gesellschaft“[7] nicht werden realisieren lassen. Vielmehr wird die Sicherheit des Einzelnen vor dem Staat und den Informationsinteressen privater Unternehmen deutlich abnehmen.

Dessen ungeachtet hat sich im Berichtsjahr die bereits in den Vorjahren beobachtete Tendenz[8] fortgesetzt, die Befugnisse der Sicherheitsbehörden vor allem durch Entscheidungen des Bundesgesetzgebers immer weiter auszudehnen. In dem Bestreben, präventiv Terroranschläge von vornherein zu verhindern, werden Eingriffsbefugnisse immer weiter ins Vorfeld konkreter Gefahren oder Straftaten ausgedehnt. Unverdächtige Bürger können immer weniger erkennen, unter welchen Voraussetzungen sie Objekte staatlicher Überwachung werden. Auch fehlt es an kompensierenden Regelungen, die die ausufernde Überwachung durch Transparenz, Auskunfts- und Korrekturrechte der Betroffenen und Löschungsfristen zumindest partiell begrenzen könnten.

Dies ist in gleicher Weise auf europäischer Ebene zu beobachten, wo permanent die Zusammenarbeit der Sicherheitsbehörden intensiviert wird, ohne dass substantielle Fortschritte bei der Erstreckung des Datenschutzes auf die sog. Dritte Säule (Zusammenarbeit der Mitgliedstaaten in den Bereichen Justiz und Inneres) erkennbar wären. Diese Erstreckung ist aber umso wichtiger, als der Europäische Gerichtshof in seiner Entscheidung vom Mai 2006 zum Transfer der *Flugpassagierdaten*[9] in die USA den Anwendungsbereich der Datenschutzrichtlinie von 1995 so drastisch eingeschränkt hat, dass möglicherweise der Zugriff außereuropäischer staatlicher Stellen auf private Datensammlungen für Zwecke der Strafverfolgung keiner datenschutzrechtlichen Kontrolle mehr unterliegt. Auch der im Berichtszeitraum in Kraft getretene Vertrag von Prüm[10], der den gegenseitigen grenzüberschreitenden Online-Zugriff der Sicherheitsbehörden in sieben EU-Mitgliedstaaten (Belgien, Deutschland,

In diesem Zusammenhang sollte aber auch erwähnt werden, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit dem Vertrag „ins-

---

[6] dazu näher unter 10.1.2

[7] Diese Aussage des Parl. Staatssekretärs im Bundesministerium der Justiz, Alfred Hartenbach, die er auf den Vorschlag einer DNA-Analyse aller männlichen Bundesbürger bezogen hat, gilt in diesem Zusammenhang in gleicher Weise.

[8] zuletzt JB 2005, 1.2

[9] vgl. 8.1

[10] BGBl. II, 626; Ausführungsgesetz v. 10. Juli 2006, BGBl. I, 1458

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Frankreich, Luxemburg, Niederlande, Österreich und Spanien) auf DNA-Datenbanken, Fingerabdruckdateien und Fahrzeugregister erlaubt, kann einen allgemeinen Datenschutzstandard für die Sicherheitsbehörden in Europa gerade auch für ihre Kommunikation etwa mit US-Behörden nicht ersetzen.

gesamt gesehen […] einen hohen datenschutzrechtlichen Standard“ bescheinigt, der gleichwohl noch verbesserungswürdig sei (Zeitschrift „Datenschutz und Datensicherheit“, Ausgabe 30/2006, S. 691–693: Peter Schaar: Datenaustausch und Datenschutz im Vertrag von Prüm).

Auf EU-Ebene wird derzeit ein „Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden“, vorbereitet.

Auf der positiven Seite der Datenschutzbilanz für 2006 stehen erneut zwei Entscheidungen des Bundesverfassungsgerichts. Mit der Entscheidung vom April 2006 zur polizeilichen *Rasterfahndung*[11] hat das Gericht die Reihe von Entscheidungen fortgesetzt, in der es – nahezu im Jahresrhythmus – seit 2003 immer wieder Maßnahmen des Gesetzgebers als verfassungswidrig beanstandet hat, die zuvor schon von den Datenschutzbeauftragten als unverhältnismäßig kritisiert worden waren. Dazu zählen der *Große Lauschangriff* ebenso wie die präventiv-polizeiliche Telekommunikationsüberwachung. Vielleicht sollte der Gesetzgeber auf Bundes- und Landesebene vor weiteren Gesetzesverschärfungen gerade im Sicherheitsbereich die Argumente der Datenschutzbeauftragten etwas ernster nehmen, um spätere Niederlagen vor dem Bundesverfassungsgericht zu vermeiden. Denn das Bundesverfassungsgericht hat den Datenschutzbeauftragten die Aufgabe des *vorbeugenden Grundrechtsschutzes* zugewiesen. Damit ist auch die eingangs gestellte Frage nach der Aufgabe von Datenschutzbeauftragten in der heraufziehenden Überwachungs- und Präventionsgesellschaft beantwortet.

In seiner Entscheidung vom April 2006 hat das Bundesverfassungsgericht die Rasterfahndung als verdachtslosen Grundrechtseingriff von großer Streubreite bezeichnet, der geradezu der Verdachtsgewinnung dient. Derartige Eingriffe dürfen die Polizeigesetze nur vorsehen, wenn sie zur Abwehr einer konkreten Gefahr für hochrangige Rechtsgüter wie den Bestand des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person auch tatsächlich erforderlich sind. Im Vorfeld der Gefahrenabwehr ist die Rasterfahndung unzulässig. Das Berliner Landesrecht genügt dieser Mindestanforderung, weil es eine gegenwärtige Gefahr für hochrangige Rechtsgüter vorsieht (§ 47 ASOG) . Diese Schwelle müssen die Polizeibehörden und die Rechtsprechung beachten. Vor dem Rasterfahndungsbeschluss hatte auch die Rechtsprechung in Berlin die Wahrscheinlichkeitsschwelle einer konkreten Gefahr relativiert, indem sie die Anforderungen an die Gefahrenwahrscheinlichkeit umso stärker senkte, je höherrangiger das Schutzgut und je

Es trifft zu, dass das Berliner Landesrecht den in der Bundesverfassungsgerichtsentscheidung zur Rasterfahndung dargelegten Anforderungen genügt, indem es eine gegenwärtige Gefahr für hochrangige Rechtsgüter fordert. Um eine verfassungskonforme Auslegung durch die Berliner Gerichte sicher zu stellen, bereitet der Senat eine Ergänzung des § 47 Abs. 1 Satz 1 ASOG vor, mit der klargestellt werden soll, dass die gegenwärtige Gefahr auch konkret sein muss, d.h. Tatsachen vorliegen müssen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge, ergibt.

[11] Beschluss v. 4. April 2006 – 1 BvR 518/02, NJW 2006, 1939

größer der zu erwartende Schaden sei. Dies ist nach der Entscheidung des Bundesverfassungsgerichts nicht verfassungskonform.

Die zweite bemerkenswerte Entscheidung des Bundesverfassungsgerichts betrifft den nicht-öffent-lichen Bereich. Mit einem Beschluss vom 23. Oktober 2006 hat das Gericht die Stellung von Versicherungskunden gestärkt[12]. Künftig müssen sie es nicht mehr hinnehmen, dass eine Versicherung sie im Leistungsfall dazu auffordert, pauschal alle behandelnden Ärzte von ihrer Schweigepflicht zu entbinden. Der Staat muss dafür sorgen, dass dem Kunden auch in dieser Situation zumindest die Möglichkeit des *informationellen Selbstschutzes* gegeben wird. Im konkreten Fall muss er also wählen können, ob er statt einer pauschalen Entbindung von der Schweigepflicht einzelne Ärzte dazu ermächtigt, bestimmte Auskünfte zu geben.

Hervorzuheben sind in diesem Zusammenhang auch zwei weitere Aussagen des Bundesverfassungsgerichts, die von grundsätzlicher Bedeutung sind: Zum einen hat es eine Schutzpflicht des Staates für die Vertragspartei betont, die nicht einfach vom Vertragsschluss absehen kann, weil die angebotene Leistung von erheblicher Bedeutung zur Sicherung ihrer persönlichen Lebensverhältnisse ist. Der überlegene Vertragspartner (hier: das Versicherungsunternehmen) kann in einer solchen Situation die Datenpreisgabe nicht unter Hinweis auf den „freiwilligen“ Vertragsschluss einfordern, sondern muss zumindest datenschutzgerechte Alternativen anbieten. Zum anderen hat das Bundesverfassungsgericht kritisiert, dass auf dem Versicherungsmarkt (und das gilt in gleicher Weise auch für andere Dienstleistungen) bisher kein Wettbewerb über die datenschutzrechtlichen Konditionen herrsche. Auch deshalb bestehe für den Versicherungskunden keine echte Vertragsfreiheit, weil für ihn die Versicherungsbedingungen letztlich nicht verhandelbar seien. Positiv gewendet wird es jetzt darum gehen, den Gedanken des Wettbewerbs um datenschutzfreundliche Dienstleistungen in der Wirtschaft, aber auch in der Gesetzgebung, etwa durch die überfällige Verabschiedung eines *Datenschutz-Audit-Gesetzes*, wieder stärker in den Vordergrund zu stellen.

1. Technische Rahmenbedingungen

1.1. Entwicklung der Informationstechnik

Verbreitung der *Informationstechnik* in Deutschland und Europa

Erstmals veröffentlichte das Statistische Bundesamt in seinen Statistischen Jahrbüchern 2006 Zahlen von 2005 über die Nutzung der Informationstechnologie in Deutschland und Europa. Wir nehmen dies zum An-

[12] 1 BvR 2027/02

lass, die dort verbreiteten Erkenntnisse zum Stand der derzeitigen Entwicklung der *Verbreitung* von Informationstechnik den technischen Entwicklungstendenzen voranzustellen.

Danach verfügten 68,6 % aller privaten Haushalte in Deutschland im Jahre 2005 mindestens über einen Personalcomputer, was gegenüber dem Jahr 2000 eine Steigerung um 45 % bedeutete. 54,6 % der Haushalte hatten über ihre Rechner Zugang zum Internet, gegenüber 2000 eine Steigerung um weit mehr als das Dreifache. Natürlich ist der Anteil der privaten Computer- und Internet-Nutzer vom Privateinkommen abhängig, aber selbst in der niedrigsten erfassten Einkommensgruppe (Haushaltsnettoeinkommen unter 1.300 €) verfügt mehr als die Hälfte über einen PC, mehr als ein Drittel hat von zu Hause aus Zugang zum Internet. Dies zeigt, dass Computer und Internetzugang auf dem Weg zur Sozialtechnologie sind, deren Fehlen ebenso ausgrenzenden Charakter haben kann wie zum Beispiel beim Telefonanschluss oder bei Radio und Fernsehen.

Noch deutlicher wird der Trend bei der Betrachtung einzelner Personen. Danach hatten 68% der Deutschen ab dem Alter von 10 Jahren zu Hause Zugang zum Internet. Der Vergleich mit den Angaben zu den Haushalten lässt darauf schließen, dass Mehrpersonenhaushalte signifikant häufiger online sind. Dass die Anteile weiter steigen werden, zeigen folgende Zahlen: Im ersten Quartal 2005 haben 99 % der Studenten, 95 % der Schüler im Alter von mindestens 15 Jahren, 92 % der Auszubildenden und 89 % der 16–24-jährigen Deutschen das Internet genutzt. Insgesamt waren es „nur“ 61 %.

Im internationalen Vergleich liegen die Zahlen der 22 der 25 Mitgliedstaaten der Europäischen Union (keine Angaben aus Belgien, Frankreich und Malta) vor. Danach haben 2005 73 % der deutschen Privatpersonen Computer genutzt. Damit liegt Deutschland hinter Schweden (84 %), Dänemark (83 %), Niederlande (83 %), Luxemburg (77 %) und Finnland (76 %) an sechster Position, also noch im oberen Viertel. Im Internet tummelten sich in der gleichen Zeit 65 % der deutschen Privatpersonen. Damit musste Deutschland neben den Genannten auch noch dem Vereinigten Königreich den Vortritt lassen.

Insgesamt lässt sich feststellen, dass die Nutzung von Computer und Internet bereits für die große Mehrheit der Privatpersonen in Deutschland selbstverständlich ist und dass der Anteil der diese Technik nutzenden Privatpersonen weiter intensiv steigen wird. Leider gibt es noch keine Statistiken darüber, wie viele Privathaushalte oder -personen davon sich bereits mit elementaren Sicherheitsvorkehrungen wie Virenschutz, Firewalls oder Spamfilter ausgestattet haben.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Entwicklungstendenzen

Seit vielen Jahren beobachten wir die Entwicklung der Informationstechnik unter anderem aus der Sicht der bunten Werbeblättchen der Elektronikmärkte. Im Gegensatz zu früheren Jahren fällt auf, dass sog. Desktop -Computer für den Schreib-, Spiel- oder Hobbytisch kaum noch beworben werden. „In“ sind jetzt schicke Notebooks für den Hausgebrauch und multimediale Ausstattung mit Leistungs- und Anwendungsmerkmalen, die mehr auf stationären als auf mobilen Gebrauch schließen lassen.

Nach wie vor dominieren im kommerziellen oder administrativen Bereich die Client-Server-Netze als gängige Netz- und Systemarchitektur. Die Hauptlast der Datenverarbeitung tragen dabei die dezentralen Arbeitsplatzsysteme (Clients), die sich jedoch zur Sicherstellung der einheitlichen Verarbeitung zentraler Dienstleistungsrechner (Server) bedienen. Allerdings haben wir in den Vorjahren bereits darauf hingewiesen, dass ein Wandel in der System- und Netzarchitektur zu beobachten ist. Server Based Systems oder Terminal Server werden zunehmend als – allerdings noch teurere - Alternative zu Client-Server-Systemen eingesetzt. Wir haben diesen Systemen in diesem Bericht ein Schwerpunktthema gewidmet[13].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf der Frühjahrskonferenz 2006 ihren Arbeitskreis für technische und organisatorische Datenschutzfragen (AK Technik) gebeten, regelmäßig zu den Konferenzen einen Kurzbericht über aktuelle und künftige technische Entwicklungen abzugeben, um den Datenschutzbeauftragten frühzeitig die Gelegenheit zu geben, die datenschutzrechtlichen Aspekte neuer Technikentwicklungen zu erörtern.

Der aktuelle Bericht befasst sich u. a. mit folgenden zukünftig verfügbaren Technikausprägungen und Phänomenen:

Der Senat beobachtet die Entwicklungen in den im Bericht aufgeführten Themenbereichen intensiv. Den sich aus den neuen Technologien ergebenden Risiken bezüglich eines sicheren IT-Einsatzes muss durch angemessene Sicherheitsmaßnahmen begegnet werden.

- *Videoüberwachung, biometrische Identifikationsverfahren* und *RFID-Anwendungen* sind bereits heute weit verbreitet oder stehen vor ihrer breiten Einführung. Zu erwarten ist bald, dass diese Technologien *untereinander vernetzt* werden und zur Gewinnung von sehr präzisen Bewegungsprofilen von Personen herangezogen werden. So ist die Verbindung von biometrischen Verfahren, die auf der Gesichtserkennung beruhen, mit der Videoüberwachung ein weiterer Schritt zur unbemerkten Identifizierung von nicht kooperierenden Personen. Wird diese Technik kombiniert mit RFID-Chips im Besitz

[13] vgl. 2.5

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

der Beobachteten, die den Bezug zu der Person herstellen, kann der Chip die Beobachtung auslösen bzw. die Person von Kamera zu Kamera „weiterreichen".

- *Voice over IP (VoIP)* ist die Übertragung von Sprachinformationen mittels Internet Protocol (IP), also die Internet-Telefonie. Diese Variante des Telefondienstes wird bereits viel genutzt, weil sie kostengünstiger und qualitativ mindestens ebenbürtig zur klassischen Telefonie ist. Viel zu wenig bekannt ist jedoch, dass die Sicherheitsprobleme des Internets damit auch beim Telefonieren wirksam werden können[14]. Zu diesen Sicherheitsproblemen gehört, dass das Thema SPAM auch für die Internet-Telefonie relevant wird:

  Unter dem Kürzel „*SPIT*" verbirgt sich das massenweise Anrufen von VoIP-Telefonen *(Spam over IP Telefony)*, eine Weiterentwicklung der heute schon lästigen automatisierten Werbeanrufe, die allerdings im Internet wesentlich billiger eingesetzt werden kann, weil spezielle Geräte nicht gebraucht werden und die Verbindungskosten vergleichsweise gering sind. Da unerwünschte Telefonate noch lästiger sind und wegen der sofortigen Aufmerksamkeit und Reaktion noch massiver in die Privatsphäre eingreifen als E-Mails, stehen neue Herausforderungen für Sicherheitsexperten bevor, um z. B. SPIT-Filter zu entwickeln. „Datenschutz und Internet-Telefonie" war auch das Thema des Internationalen Symposiums, das wir im Rahmen der Internationalen Funkausstellung 2006 veranstaltet haben[15].

- Weiter in die Zukunft reichen die Hoffnungen der Wissenschaftler, aber auch der Anwender, die Effekte der Quantenphysik für *Quantencomputer* nutzbar zu machen, die bestimmte Aufgaben im Bereich der Verschlüsselung hocheffizient lösen können. Zu diesen Aufgaben gehört das Brechen heute üblicher Verschlüsselungsverfahren. Bereits bekannt ist ein Algorithmus, mit dem das Problem der Faktorisierung von Produkten großer Primzahlen mit geringem Aufwand gelöst werden kann und so auf dem RSA-Algorithmus basierende asymmetrische Kryptoverfahren kompromittiert werden können. Da Quantencomputer das Laborstadium so bald nicht verlassen werden, sind diese Risiken bisher noch nicht gegeben.

  Andererseits verspricht die *Quantenkryptografie* bereits die Lösung der anstehenden Probleme: Quanteneffekte konnten dazu genutzt werden, neue Formen geheimer Kommunikation zu entwickeln, bei

Besonderes Augenmerk gilt dabei der Übertragung von Sprachinformationen mittels Internet-Protokoll. Mit dieser Technologie ist es möglich, vorhandene Netzinfrastrukturen effizienter zu nutzen und neue Anwendungsformen des IT-Einsatzes für die Verwaltung zu erschließen. Voraussetzung für den Einsatz von VoIP ist die Planung und Umsetzung von anforderungsgerechten Sicherheitsmaßnahmen, um den spezifischen Risiken, wie sie vom Berliner Beauftragte für Datenschutz und Informationsfreiheit beispielhaft aufgeführt werden, wirksam begegnen zu können.

[14] Zu VoIP hat sich die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits in einer Entschließung geäußert, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005", S. 20. http://www.datenschutz-berlin.de/doc/de/konf/70/70DSBVoIP.pdf. Eine Orientierungshilfe der Konferenz zu VoIP ist in Vorbereitung.

[15] vgl. dazu 10.1.7

denen jeder Abhörversuch bemerkt und die Kommunikation abgebrochen wird, ohne dass es zu einer Preisgabe von Geheimnissen kommen kann.

- Keine bloße Zukunftsmusik sind die weitreichenden Anwendungen der *Nanotechnologie* die sich mit der Trennung, dem Zusammenbau und der Verformung von Werkstoffen in der Größenordnung von Atomen und Molekülen beschäftigt. Hier spielen die Oberflächeneigenschaften und quantenmechanische Effekte eine Rolle. In der Nanotechnolgie wird eine der wichtigsten technologischen Revolutionen der Zukunft gesehen, die weite Bereiche von Wissenschaft, Technik und Gesellschaft erfassen wird und bereits heute unter erheblichem Förderaufwand weltweit vorangetrieben wird. Wir sehen in dieser technischen Entwicklung erhebliche Risiken für die informationelle Selbstbestimmung. Wir hoffen, dass sie auch Chancen für ihre Sicherung bereithält. Deshalb haben wir uns mit dem Thema näher befasst:

Nanotechnologie

Seit Jahren ist zu beobachten, dass die weiter fortschreitende Miniaturisierung von informationstechnischen Bausteinen wie Mikroprozessoren, Speicherchips, Sensoren, Sendern, Antennen usw. nicht nur zur weiteren und stetigen Verbesserung des Preis-Leistungs-Verhältnisses gängiger informationstechnischer Systeme führt, sondern völlig neue Technologien hervorbringt, deren Konsequenzen für künftige Anwendungen und deren Implikationen für die Gesellschaft bisher nur vage vermutet werden können. Dies gilt auch für die Sicherstellung der informationellen Selbstbestimmung, für die eine allgegenwärtige Informationstechnik neuartige Herausforderungen mit sich bringen wird.

Seit längerem befassen wir uns mit der *RFID-Technologie*[16], die als Nachfolger des Barcodes im Bereich der Logistik zu starken Innovations- und Rationalisierungsschüben geführt hat. Der Hauptanwendungsbereich mag darüber hinwegtäuschen, dass auch der Datenschutz herausgefordert wird. Sobald jedoch die Verbindung logistischer oder warenwirtschaftlicher Daten mit personenbezogenen Angaben hergestellt wird, kann die einzelne Person in ihrem Verhalten transparent werden: Wer bevorzugt welche Ware? Wofür gibt wer gerne Geld aus? Was macht er nach dem Kauf? Was tut er mit der gekauften Ware? Die Antworten auf diese Fragen interessieren viele: Marketingexperten, Werbefachleute, Sicherheitsdienste, vielleicht auch Strafverfolger und Geheimdienste.

Ein neues Stichwort macht deutlich, dass über Informationstechnik in Staubgröße nachgedacht wird:

[16] zuletzt JB 2005, 2.1

Smart Dust. Es gibt die Vision von allgegenwärtigen *Sensoren*, Sendern, Mikroprozessoren, die bestimmte Informationen aufnehmen, weitergeben oder verarbeiten. Möglich wird die „staubartige“ Intelligenz durch die weltweit intensiv angestoßenen Entwicklungsprojekte im Bereich der Nanotechnologie. Ein Aktionsplan der Kommission der Europäischen Gemeinschaften für die Jahre 2005 bis 2009[17] zitiert die Erwartung von Analysten, wonach noch im laufenden Jahrzehnt ein Marktwachstum um Hunderte von Milliarden Euro bei den Nanowissenschaften und Nanotechnologien erreicht wird. Die Kommission forciert daher die Ausbildung, Forschung und Entwicklung auf diesem Gebiet nachhaltig, verlangt aber auch die Beachtung ethischer Grundsätze, die frühzeitige Berücksichtigung gesellschaftlicher Sichtweisen bei der Forschung und Entwicklung sowie die Förderung des Dialogs mit den Bürgern. Neben den Chancen für die wirtschaftliche Entwicklung spricht die Kommission auch mögliche Gesundheitsgefahren an. Als mögliche ethische Frage in Verbindung mit Nanotechnologien erwähnt die Kommission beispielhaft Eingriffe in die Privatsphäre durch unsichtbare Sensoren.

Die Entwicklung der Informationstechnik wird durch *Nanotechnologie* in verschiedener Weise vorangetrieben[18]:

- neue Speichermedien mit der vielfachen Speicherdichte heutiger Festplatten, die kostengünstig zu produzieren sind,
- Leitungsnetze mit Leitungen von der Dicke weniger Atome,
- Transistoren mit der Taktfrequenz im Terahertz-Bereich.

Entwicklungen dieser Art würden die Geschwindigkeit der Entwicklung der Computertechnologie gegen das bekannte Moore´sche Gesetz[19] noch wesentlich erhöhen
.
Die weltweiten Anstrengungen zur Entwicklung von Nanotechnologien werden von kritischen Stimmen begleitet, die den häufig unkritisch begeisterten Hoffnungen auf gewaltige medizinische Fortschritte, auf die Fortschritte beim Umweltschutz und der Entwicklung der Informationstechnologie Warnungen vor gesundheitlichen Gefahren, vor Umweltschäden und vor negativen gesellschaftlichen Implikationen entgegensetzen.

Mangels empirischer Erfahrungen mit der neuen Technologie werden in den verfügbaren Quellen, die

---

[17] Mitteilung der Kommission an den Rat, das Europäische Parlament und den Wirtschafts- und Sozialausschuss, Nanowissenschaften und Nanotechnologien: Ein Aktionsplan für Europa 2005–2009, KOM(2005) 243 endg.

[18] Eva Gutierrez für das Electronic Privacy Information Center (EPIC): Privacy Implications of Nanotechnologies, http://www.epic.org/privacy/nano/

[19] Das Moore´sche Gesetz besagt, dass sich die Leistung von Mikroprozessoren alle 18 Monate verdoppelt.

den Bezug zwischen Nanotechnologie und Datenschutz herstellen, folgende technische Entwicklungen genannt, denen sich die Datenschutzbeauftragten stellen müssen[20]:

- Die mit der Nanotechnologie bewirkte sprunghafte Verbesserung der Leistung von Prozessoren, der Kapazität von Speichern und Datenübertragungskomponenten führt zu effizienteren und wesentlich preisgünstigeren Möglichkeiten der Datengewinnung, -verarbeitung, -speicherung und –weiterleitung. Dies verbessert nicht nur die wirtschaftlichen und gesellschaftlich gewünschten Potenziale der Informationstechnik, sondern auch ihre Potenziale und Anreize zum Missbrauch der Daten oder zur weiteren Eröffnung von Anwendungen, die im Sinne der Wahrung von Persönlichkeitsrechten fragwürdig sind.

- Die Nanotechnologie eröffnet neue Möglichkeiten zur unmerklichen Beobachtung und Überwachung von Personen. Sensoren, Sender und Mikroprozessoren können beliebige Lebenssituationen registrieren, senden und festhalten. Die Personen werden manipulierbar in ihrem Verhalten, auch weil sie sich der Beobachtung und Einflussnahme von dritter Seite nicht bewusst werden. Das Eindringen in die private Sphäre erfolgt ebenso unmerkbar.

- Ein weiterer Schritt dieser Entwicklung ist die mögliche Implantation von Mikrosystemen in den Körper. Mit *RFID-Chips* ist dies bereits heute möglich, aber kaum ohne Wissen und Wollen des Betroffenen. Die Einbringung von „Smart Dust“ könnte jedoch auch ohne Wissen des Betroffenen erfolgen.

- Die Nanotechnologie fördert die Konvergenz zwischen verschiedenen Technologien und Wissensgebieten mehr als dies bisher schon der Fall ist. Nanotechnologie, Biologie, Medizin, Informationstechnologie und kognitive Wissenschaften rücken einander näher, fördern neue Mischtechniken und werfen erhebliche ethische Fragen auf, die allgemein den Schutz der menschlichen Selbstbestimmung betreffen, von der die informationelle Selbstbestimmung einen Teil darstellt.

1.2 Datenverarbeitung in der Berliner Verwaltung

Leider hält das Statistische Jahrbuch 2006 keine Daten für die Bundesländer bereit, sodass nicht festgestellt werden kann, wo Berliner Bürger und Unternehmen im nationalen Vergleich der Nutzung von Computern und Internet stehen. Aussagen zur Datenverarbeitung in Berlin lassen sich daher nur für die Berliner Verwaltung treffen, weil gesetzliche Unterrichtungs-

[20] P. Lemoine, Commission National de l`Informatique et des Libertés, Frankreich: Nanotechnologies and Data Protection, http://www.cnil.fr/fileadmin/documents/uk/Ph_Lemoine_nanos_janvier_06_VAVD.pdf

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

pflichten insoweit einen Überblick über die aktuelle Entwicklung erlauben.

§ 24 Abs. 3 Satz 3 Berliner Datenschutzgesetz verpflichtet die Berliner Behörden, uns über neue IT-Projekte und wesentliche Änderungen bestehender Projekte zu unterrichten. Dieser Pflicht wird zwar nicht immer und vor allen Dingen nicht immer rechtzeitig und gründlich nachgekommen, sodass eine Beratung in datenschutzrechtlicher oder technisch-organisatorischer Hinsicht nicht immer umfassend geleistet werden kann.

Die Senatsverwaltung für Inneres und Sport wird die Verantwortlichen für IT-Projekte nochmals auf die bestehenden Pflichten zur Beteiligung des Berliner Beauftragten für Datenschutz und Informationsfreiheit und auf die notwendigen inhaltlichen Informationen hinweisen.

Zunehmend erfolgt die Unterrichtung unter Beifügung von professionell erstellten Sicherheitskonzepten. Dies ist sehr zu begrüßen, geben uns die Konzepte doch einen umfassenden Überblick über die Maßnahmen, die zur Absicherung eines ordnungsgemäßen und sicheren Verfahrensbetriebs ergriffen worden sind. Erstaunlicherweise ist der Trend festzustellen, die inhaltliche Ausgestaltung der Verfahren dafür nur noch sehr unpräzise zu beschreiben. Welche Daten wie wozu aufgrund welcher Rechtsgrundlagen verarbeitet werden, bleibt immer häufiger wolkig. Eine datenschutzrechtliche Bewertung ist mangels Informationen immer häufiger erst nach langen Rückfragen möglich, häufig genug nicht vor der Inbetriebnahme der Verfahren.

IT-Politik für die Berliner Verwaltung – die prioritären Projekte

Im Vorjahr haben wir an dieser Stelle über wesentliche Veränderungen in der IT-Politik des Landes berichtet. Diese IT-Politik soll Berlin fit machen für die Herausforderungen, die sich in naher Zukunft stellen. Moderne Fachverfahren sollen einerseits den heftigen Personalabbau kompensieren, gleichzeitig die Verwaltungsabläufe beschleunigen, die Arbeitszufriedenheit erhöhen und den Kunden, also den Bürgern und Unternehmen des Landes, aber auch den eigenen Mitarbeitern moderne Verwaltungsdienstleistungen anbieten. Die Schwerpunkte aller Bemühungen finden sich im Zusammenhang mit dem Stichwort „*E-Government*“. Es geht darum, über das Internet Verwaltungsdienstleistungen online – und dennoch sicher - anzubieten. Bürger und Unternehmen sollen vom eigenen Computer aus zunehmend Leistungen der Verwaltung in Anspruch nehmen können – vom einfachen Abruf von Formularen bis hin zu komplexen Anträgen.

Um die Rahmenbedingungen für das Erreichen dieser Ziele zu erreichen, wurden im Vorjahr neun prioritäre Projekte begonnen. Diese Projekte wurden in diesem Jahr fortgesetzt und ergänzt. Einige Projekte wurden sogar erfolgreich abgeschlossen. Im Folgenden berichten wir über den Stand der Projekte.

- Die *Landesvereinbarung zu Dienstleistungen im Be-*

Durch die Einführung des Berlin-Telefons über das

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats
reich der Sprach- und Telekommunikation ist zwischen der Senatsverwaltung für Inneres und dem IT-Dienstleistungszentrum (ITDZ) mittlerweile abgeschlossen worden. Das landesweite Call-Center „Berlin-Telefon“ ist in noch eingeschränkter Form – weil noch nicht alle Behörden darüber erreicht werden können - in Betrieb gegangen.	Call-Center des IT-Dienstleistungszentrum Berlin (ITDZ) verfügt die Berliner Verwaltung über eine zentrale Einwahlnummer zur Berliner Verwaltung („900“). Ausgehend von den damit vorhandenen guten techni-schen und organisatorischen Vorraussetzungen strebt die Senatsverwaltung für Inneres und Sport eine Beteiligung Berlins an dem Projekt einer bundesweiten Einwahl-Plattform an. Die für E-Government zuständigen Staatssekretäre des Bundes und der Länder ha-ben in ihrer Sitzung am 19.03.2007 beschlossen, die-ses Vorhaben als prioritäres Projekt in den bestehen-den Aktionsplan Deutschland Online aufzunehmen.
- Das Projekt *ProBetrieb* hat das Ziel, Grundsätze für den Betrieb der Informationstechnik (Betriebskonzepte, Betriebssysteme, Architekturen) in der Berliner Landesverwaltung aufzustellen. Sie sollen auf dem weltweit anerkannten ITIL-Standard (Information Technology Infrastructure Library) und auf den IT-Organisationsgrundsätzen aufbauen. Ergebnis soll eine Art „Projektmanagementhandbuch“ sein. Das Projekt ist noch nicht abgeschlossen.	Das Projekt ProBetrieb hat mit den praktischen Arbeiten begonnen. Ziel des Projektes ist die Erarbeitung von Grundsätzen für einen effizienten IT-Infrastrukturbetrieb für die Berliner Verwaltung. Das Projekt soll September 2007 beendet sein.
- Die Entwicklung eines einheitlichen interaktiven Formularservices im Rahmen des Projekts *ProForm* ist ebenfalls noch nicht abgeschlossen. Dabei wurde zunächst auf eine Zusammenarbeit mit dem Land Brandenburg gesetzt, das eine entsprechende Lösung erprobt. Inzwischen wird jedoch eine Ausschreibung erwogen.	Fachkonzept und Abschlussbericht zur Voruntersuchung des Projektes ProForm liegen vor. Die dort enthaltenen Handlungsempfehlungen bilden die Basis für die weitere Projektarbeit.
- Ein wichtiger Basisdienst für das E-Government ist ein zentraler Druck- und Versanddienst im ITDZ, mit dem die Ergebnisse der Fachverfahren abgestimmt und einheitlich dargestellt werden. Dieses Projekt *ProOutput* hat ein Outputmagament erarbeitet, welches in einer Pilotanwendung für das Fachverfahren ISBJ (Informationssystem Berliner Jugendhilfe) bereits erprobt wird.	Das als E-Government-Dienst des ITDZ Berlin verfügbare Outputmanagement wird im Rahmen vom Projekt ISBJ erfolgreich genutzt.
- Das Projekt *Virtuelle Poststelle* ist für den Datenschutz von besonderem Interesse, denn damit soll der elektronische Zugang von Kunden (Bürger, Unternehmen) zur Verwaltung eingerichtet werden. Dabei müssen die technisch-organisatorischen Datenschutzziele der Vertraulichkeit, Integrität und Authentizität der elektronischen Postsendungen gewährleistet werden. Dies bedeutet, dass auch Dienste zur Verschlüsselung, elektronischen Signatur und zur elektronischen Zeitstempelung angeboten werden müssen. Realisiert werden sollen diese Sicherheitsdienste mit dem Produkt GOVERNIKUS der Firma Bremen Online-Services GmbH & Co KG, die für den erfolgreichen Bremer Beitrag zum MEDIA@Komm-Wettbewerb verantwortlich war. Inzwischen hat das ITDZ ein Pilotprojekt im Bereich der Berliner Sicherheitsbehörden initiiert.	Zum landesweiten Einsatz der virtuellen Poststelle wird derzeit der Abschluss einer Landesvereinbarung gemäß VV IT-Steuerung zwischen der Senatsverwaltung für Inneres und Sport und dem ITDZ Berlin vorbereitet.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- Für das *Senats-Informations- und Dokumentationssystem* (*SIDok*) wurden nach einem Teilnahmewettbewerb vier Unternehmen zur Abgabe eines Angebots aufgefordert und der Zuschlag inzwischen erteilt. 2007 wird der Probebetrieb begonnen, später erfolgt der Roll-Out mit 300 Lizenzen. Eine Entscheidung für das landesweite Dokumentenmanagement- und Vorgangsbearbeitungssystem wurde damit noch nicht getroffen. Dazu erfolgt derzeit noch die Klärung der Ziele und Vorgehensweisen.

  Zu den datenschutzrechtlichen Aspekten solcher Dokumentenmanagementsysteme verweisen wir auf die Ausführungen im Schwerpunktthema unter 2.6.

- Die *IT-Organisationsgrundsätze* sind in diesem Jahr vom Senat beschlossen worden. Sie legen fest, auf welchen Grundstrukturen der IT-Einsatz in der Berliner Verwaltung erfolgt. Dazu gehören insbesondere die *IT-Fachverfahren* und *IT-Querschnittsverfahren* (hier zu nennen die Verfahren für das Berliner Rechnungswesen und die Personalverwaltung), die (künftigen) *IT-Dienste* wie die elektronische Vorgangsbearbeitung, elektronische Zahlungsverfahren, Formularservices, Verschlüsselung, elektronische Signatur, virtuelle Poststelle, Intranet, Internet usw. sowie die *IT-Infrastruktur* vom einzelnen Gerät bis zum landesweiten Netz. Sie legen ferner die Abstimmungs- und Entscheidungswege fest und ordnen die Verantwortung und Aufgaben bei IT-Maßnahmen Rollen zu, die von einzelnen Personen oder Organisationseinheit wahrgenommen werden.

- Das Projekt *Standards und Normen* hatte sich zum Ziel gesetzt, mehr oder weniger verbindliche Verabredungen zu treffen, um einen informationstechnischen Wildwuchs mit konkurrierenden und inkompatiblen Lösungen zu verhindern, wie er in der Vergangenheit in Teilbereichen nicht immer ausgeschlossen werden konnte.

  Im Ergebnis hat der Senat im August 2006 IT-Standardisierungsgrundsätze beschlossen, mit denen die jährliche Festlegung von IT-Standards der Berliner Verwaltung geregelt werden soll. Zielrichtung der Standardisierung ist die Beschränkung der eingesetzten IT-Komponenten und eine Vereinheitlichung der im Land eingesetzten Systeme. Die Standards sollen Voraussetzungen für das Zusammenwirken und die Austauschbarkeit unterschiedlicher IT-Systeme schaffen, die Wiederverwendbarkeit vorhandener Komponenten unterstützen, IT-Verfahren und IT-Infrastrukturen entkoppeln und die Nutzung verfahrensübergreifender Dienste vorantreiben. Damit leisten sie einen Beitrag zur Investionssicherheit.

  Es gibt Standards, die als verbindlich deklariert und damit ohne Ausnahme anzuwenden sind. Sofern ei-

ne solche verbindliche und eindeutige Festlegung (noch) nicht sinnvoll ist, wird die Anwendung von Standards nur empfohlen, was immerhin bedeutet, dass ein Abweichen von diesen empfohlenen Standards nur in begründeten Fällen erlaubt ist. Soweit auch solche relativierte Festlegungen (noch) nicht sinnvoll sind, können Standards als „unter Beobachtung“ klassifiziert werden.

Sofern Verwaltungen von den vorgegebenen Standards abweichen, muss der eventuell dadurch entstehende Mehraufwand von ihnen getragen werden. Die IT-Standards der Berliner Verwaltung wurden erstmals für das Jahr 2007 festgelegt. Verbindliche Standards sind in den Fällen formuliert worden, in denen der Bund für sich verbindliche Regelungen geschaffen hat. Ferner sind Standards für verbindlich erklärt worden, in denen sich welt-, europa- oder deutschlandweit bereits Einvernehmen zur einheitlichen Verwendung herausgebildet hat. Dazu zählen beispielsweise die Extensible Markup Language (XML) für die Datenbeschreibung und zum Datenaustausch, DOMEA 2.1 für das Dokumentenmanagement, TIFF für grafische Textformate, PDF für Textdokumente im Internet oder für Dokumente, die nicht weiterverarbeitet werden müssen, JPEG für den Austausch von Bildern, OSCI und Governikus für sichere Abwicklung von Transaktionen im Rahmen von E-Government-Anwendungen, File Transfer Protokoll (ftp) für die Übertragung von Dateien und SQL 2 als Abfrage-, Verarbeitungs- und Definitionssprache für relationale Datenbanken.

Für die IT-Sicherheit wurden diverse verbindliche oder empfohlene Standards definiert, deren Beachtung ganz sicher für die vertrauenswürdige Datenverarbeitung und ein verlässliches E-Government Voraussetzung sein wird. Wir gehen darauf später in diesem Abschnitt ein.

- Die Umlegung der Kosten des IT-Einsatzes auf die teilnehmenden Verwaltungen soll in dem Projekt *Finanzierungskonzept* geregelt werden. Dieses Projekt hat noch nicht begonnen.

Mit dem Projekt zur Entwicklung eines *Virtuellen Bürgeramtes* ist im Berichtsjahr begonnen worden. Der Projektauftrag für die Voruntersuchung (Machbarkeitsstudie) für das Online-Bürgeramt sieht vor, dass der Staatssekretärsauschuss zur Steuerung der Verwaltungsmodernisierung bis Ende Juni 2007 eine Entscheidungsvorlage zur Realisierung des Projekts erhält, das u. a. auf den prioritären Projekten und den vorhanden Fach- und Querschnittsverfahren aufbaut.

Das virtuelle Bürgeramt soll den Bürgern des Landes über das Internet alle wesentlichen Informationen zu den Dienstleistungen an einer Stelle erschließen und ihnen die Möglichkeit bieten, online bei einer zentralen Stelle elektronische Anträge für alle Bürgeranlie-

Für die Inanspruchnahme der Dienstleistungen der Bürgerämter ist in vielen Fällen die Schriftform vorgeschrieben. Bei einem solchen Schriftformerfordernis müsste ein Antragsteller seinen Antrag eigenhändig unterschreiben. Bei der Abwicklung über das Internet hingegen ist in diesen Fällen die Verwendung einer qualifizierten digitalen Signatur notwendig. Nur qualifizierte elektronische Signaturen werden im elektronischen Rechtsverkehr der eigenhändigen Unterschrift gleichgestellt.

Die Verwendung von qualifizierten elektronischen Signaturen hat sich im elektronischen Rechtsverkehr flächendeckend noch nicht durchgesetzt. Als technische Lösung für den Einsatz qualifizierter elektronischer

gen zu stellen. Die medienbruchfreie Bearbeitung solcher Anträge setzt bei gesetzlichem Schriftformerfordernis die Verwendung der qualifizierten elektronischen Signatur voraus. Da die notwendigen Signaturkarten in der Bevölkerung noch nicht verbreitet sind, wird sich das Angebot zunächst auf Anträge beschränken müssen, bei denen auf eine digitale Signatur verzichtet werden kann. Zumindest kann den Bürgern die Möglichkeit gegeben werden, über den Formularservice des Berlin-Portals berlin.de Antragsdaten elektronisch zu übermitteln.

IT-Sicherheit in Berlin

Die Verpflichtung der verantwortlichen Stellen, die Datenverarbeitung ordnungsgemäß und sicher zu betreiben, ist seit jeher in den deutschen Datenschutzgesetzen verankert. Sowohl private Unternehmen, die dem Bundesdatenschutzgesetz unterliegen, als auch öffentliche Stellen in Berlin, die das Berliner Datenschutzgesetz zu beachten haben, müssen die personenbezogenen Daten (aber auch andere schutzwürdige Daten, die nicht dem Datenschutz unterfallen) so verarbeiten, dass ihre Vertraulichkeit, Korrektheit und Authentizität gewährleistet werden können. Die Daten und die sie verarbeitenden Systeme müssen verfügbar und die Datenverarbeitung transparent und nachvollziehbar sein.

Die Pflicht zur Umsetzung technischer und organisatorischer Maßnahmen beschränkt sich zwar nicht nur auf diese Ziele, sondern schließt vor allem auch ein, dass die Datenschutzrechte der Betroffenen effizient umgesetzt werden können, z. B. das Recht auf Auskunft sowie die Berichtigung, Löschung und Sperrung von Daten. „Insbesondere“ – so die Gesetze – sind jedoch Maßnahmen zu ergreifen, die der Ordnungsmäßigkeit und Sicherheit dienen.

Nachdem bereits zu Beginn 1999 in Berlin eine Richtlinie[21] erlassen wurde, die die Behörden dazu verpflichtet, die IT-Sicherheit ihrer Systeme und Verfahren sicherzustellen, und dazu auch methodische Vorgaben zur Entwicklung von IT-Sicherheitskonzepten machte, wurde mit der Novellierung des Berliner Datenschutzgesetzes im Jahre 2001 die Forderung ins Gesetz geschrieben, dass vor der Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung die zu treffenden technischen und organisatorischen Maßnahmen, die den oben beschriebenen Sicherheitszielen dienen, auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln sind (§ 5 Abs. 3 Satz 1 BlnDSG).

Signaturen ist bislang die Verwendung von Signaturkarten mit entsprechenden Kartenlesegeräten bekannt.

Das Projekt Virtuelle Bürgerdienste setzt bei dem Einsatz von qualifizierten elektronischen Signaturen und technischen Lösungen auf die künftigen Entwicklungen des Bundes. Mit der Einführung des elektronischen Personalausweises ab dem Jahr 2008 wird die weitere Verbreitung der qualifizierten digitalen Signatur und entsprechender Infrastruktur erwartet. Das Virtuelle Bürgeramt wird diese Entwicklung aufgreifen und anstreben, Dienstleistungen mit Schriftformerfordernis auf der Grundlage des elektronischen Personalausweises abzuwickeln.

[21] Richtlinie zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung – IT-Sicherheitsrichtlinie – v. 5. Januar 1999, DBl. I, 5

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

In den Festlegungen der IT-Standards 2007 auf der Grundlage der neuen IT-Standardisierungsgrundsätze finden sich auch zahlreiche Vorgaben für die Sicherstellung der IT-Sicherheit, die die IT-Sicherheitsrichtlinie aktualisieren und die dazugehörigen IT-Sicherheitsstandards modernisieren und ergänzen:

- Verbindlich wurde geregelt, dass Sicherheitskonzepte nach dem IT-Grundschutzkatalog des BSI und den BSI-Standards 100-1, 100-2 und 100-3[22] zu erstellen sind. Damit wird dem veränderten Ansatz beim IT-Grundschutz Rechnung getragen, auf die Methodik des IT-Sicherheitshandbuchs[23] von 1992 fortan auch bei der Risikoanalyse zu verzichten und in den Fällen, in denen eine Schutzbedarfsanalyse mehr als normalen Schutzbedarf ergibt, besondere Risikoanalysen nach BSI-Standard 100-3 durchzuführen[24]. Mit dieser verbindlichen Regelung werden auch die methodischen Vorgaben der IT-Sicherheitsrichtlinie angepasst, die die bedarfsweise Anwendung des IT-Sicherheitshandbuchs noch vorsah.

  Empfohlen wird ferner die Verwendung des modellhaften Sicherheitskonzepts (ModellSiko) für die Behörden der Berliner Verwaltung zur vereinfachten Erstellung von Sicherheitskonzepten. Dies ist kein Widerspruch zur verbindlichen Empfehlung der Nutzung des Grundschutzkatalogs des BSI, denn das ModellSiko ist auf der Grundlage des Grundschutzkatalogs entstanden, berücksichtigt aber bereits die Rahmenbedingungen in der Berliner Verwaltung, also die bestehenden Regelungen und Standards sowie die bereits als Sicherheitsinfrastruktur vorhandenen Maßnahmen wie das Sicherheitsrechenzentrum des ITDZ, das vorhandene Angebot an Verschlüsselungsverfahren im Berliner Landesnetz sowie die Schutzmaßnahmen im Grenznetz zwischen dem Intranet der Berliner Verwaltung und dem Internet.

- Verbindlich wurde für die Nutzung des Internets und der Fremdnetze außerhalb des Geltungsbereichs der IT-Sicherheitsrichtlinie vorgegeben, dass dafür ein schlüssiges Sicherheitskonzept erarbeitet und konsequent umgesetzt sein muss. Der Übergang in solche Netze soll nur über das Grenznetz des ITDZ erfolgen. Wenn dies ausnahmsweise nicht möglich ist, müssen gleichwertige Sicherheitsmaßnahmen in Abhängigkeit vom eigenen Schutzbedarf realisiert werden.

---

[22] http://www.bsi.bund.de/gshb/index.htm

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0 v. März 1992

[24] Ob das sinnvoll ist, müssen spätere Erfahrungen mit der Risikoanalyse auf der Basis IT-Grundschutz zeigen. Es gibt Hinweise, wonach die neue Methodik bei ungewöhnlichen IT-Verfahren, die kaum mit den Grundschutzkatalogen zu beschreiben sind, im Gegensatz zum IT-Sicherheitshandbuch nicht flexibel genug angewendet werden kann, um sichere Ergebnisse zu erzielen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- Wegen der besonderen Risiken des unkontrollierten Datenabflusses wird empfohlen, auf die Nutzung aktiver Komponenten unter Active X zu verzichten. Arbeitsplätze mit Zugang zum Internet, die aktive Komponenten benötigen, sollen physisch oder logisch vom lokalen Netz getrennt betrieben werden.

- Der Einsatz von gestaffelten Virenschutzmaßnahmen ist verbindlich vorgeschrieben. Sie sind in mehreren Ebenen als Bestandteil der zentralen als auch der dezentralen Infrastruktur einzusetzen. Es wird empfohlen, für den Virenschutz in dezentralen Systemen Scanner einzusetzen, die entweder auf Befehl des Benutzers (On-Demand) oder ständig im Hintergrund (On-Access) aktiv sind.

- Daten mit hohem Schutzbedarf sind grundsätzlich verschlüsselt zu übertragen, es sei denn, es werden gleichwertige Alternativen gefunden. Es wird empfohlen, dafür den Standardnetzzugang des ITDZ zu nutzen.

  Zu dieser Forderung ist festzustellen, dass im Berliner Landesnetz im Sinne des Standards grundsätzlich alle personenbezogenen Daten als solche mit hohem Schutzbedarf anzusehen sind. Wir gehen davon aus, dass deshalb die Verschlüsselung (oder Gleichwertiges) bei der Übertragung personenbezogener Daten obligatorisch ist.

Die konkrete Schutzbedarfsfeststellung für einen geplanten IT-Einsatz ist Aufgabe des IT-Verfahrensverantwortlichen und bildet die Voraussetzung für die Auswahl geeigneter Sicherheitsmaßnahmen und die Erstellung eines IT-Sicherheitskonzeptes. Bei personenbezogenen Daten kann grundsätzlich von einem hohen Schutzbedarf ausgegangen werden.

- Für die sichere Datenübertragung in einer Kommunikationsverbindung mit einem WebServer im Intranet wird der Einsatz von SSL/TLS empfohlen, sofern der Standardnetzzugang nicht benutzt wird.

- Für die symmetrische Verschlüsselung wird die Verwendung der Algorithmen AES und 3DES empfohlen.

- Der Einsatz von Firewalls ist sowohl in der zentralen als auch in der dezentralen IT-Infrastuktur verbindlich. Die Zugangs- und Zugriffregeln sollen alle Zugänge und Zugriffe ausschließen, die nicht explizit erlaubt sind.

- Fernwartung ist nur zulässig, wenn besondere Schutzmaßnahmen getroffen worden sind.[25]

- Auf Laufwerke für externe Datenträger ist verbindlich zu verzichten, sofern diese über einen Anschluss an das Berliner Landesnetz verfügen. Zumindest ist der Zugriff auf Schnittstellen für Wechselmedien zu sperren, sofern ihre Nutzung nicht für die Aufgabenerfüllung zwingend erforderlich ist.

[25] Bei der Fernwartung sind die Anforderungen aus § 3 a BlnDSG zu beachten.

- Um zu verhindern, dass neue IT-Verfahren und Programme die Sicherheit freigegebener Verfahren beeinträchtigen, ist das Zusammenwirken von Verfahren mit freigegebenen Verfahren im verfahrensspezifischen Sicherheitskonzept verbindlich zu berücksichtigen. Sofern die IT-Verfahren die zentrale IT-Infrastruktur nutzen, sind die dafür verwendeten Kommunikationsprotokolle und -dienste aufzulisten und in die Risikobetrachtung für das verfahrensspezifische Sicherheitskonzept einzubeziehen. Es ist ferner für IT-Verfahren verbindlich vorgesehen, dass die Anwender der Verfahren keine lokalen Administratorrechte benötigen.

- Für die elektronische Signatur werden nur *Smartcards* nach dem Standard ISO/IEC 7816 empfohlen. Als Algorithmen sollen nur solche verwendet werden, die von der Bundesnetzagentur empfohlen werden. Diese erfüllen jedenfalls die Anforderungen des Signaturgesetzes.

Aktuelle IT-Projekte des Landes

Im Berichtsjahr wurde wieder eine Reihe von neuen IT-Projekten begonnen, die sich derzeit in unterschiedlichen Stadien der Entwicklung und Einführung befinden.

Das *Polizeiliche Informations- und Kommunikationssystem POLIKS*, bei dem wir 2005 noch Anfangsschwierigkeiten feststellten, ist im Berichtsjahr erfreulicherweise aus den Schlagzeilen gekommen, was darauf hindeutet, dass ein zufrieden stellender Betrieb des Verfahrens möglich war. Demnächst wird die Datenverarbeitung der Polizei durch das neue Verfahren zur „Computergestützten Anwendung für Sachbearbeitung und Auswertung“ (*CASA*) ergänzt. Mit diesem Verfahren sollen komplexe Struktur- und Ermittlungsverfahren unterstützt werden, indem Daten und unterschiedliche Quellen und Ermittlungsverfahren für repressive und präventive Zwecke zusammengeführt werden können. So können Zusammenhänge festgestellt werden, die bei der bisherigen Verarbeitung der Daten nicht erkannt werden konnten. Das Verfahren soll im Bereich der Terrorismusabwehr, der Verfolgung organisierter Kriminalität sowie der schweren Wirtschaftskriminalität und der Hinweisbearbeitung bei spurenintensiven Verfahren eingesetzt werden. Schwerpunkt der noch anhaltenden datenschutzrechtlichen Begleitung ist die Sicherstellung der Zweckbindung der dort aus unterschiedlichen polizeilichen Quellen verarbeiteten Daten.

Die Berliner Polizei hat im Dezember 2006 ein Testcenter für das geplante Vorhaben CASA eingerichtet. Im Rahmen der Pilotphase des Produkts werden auch die noch offenen datenschutzrechtlichen Fragen zu klären sein.

Auch der Verfassungsschutz will seine Arbeit mit Verfahren unterstützen, die Bezüge zwischen den verschiedenen Objekten seiner Beobachtungen automatisch herstellen können. Die Amts- und Analysedatei (*AMANDA*) beruht auf einem bereits beim bayerischen Verfassungsschutz eingesetzten Standardprogramm, welches das Konzept der Wissensnetze praktisch an-

wendet. Das von uns geprüfte Sicherheitskonzept für AMANDA entspricht den hohen Erwartungen, die angesichts des besonders strikten Schutzbedarfs anzulegen waren.

Nachdem die Daten zu Verkehrsordnungswidrigkeiten seit einiger Zeit von der Polizei mit dem neuen Verfahren BOWI21 verarbeitet werden, sollen in der Verfahrensverantwortung des Ordnungsamtes des Bezirks Friedrichshain-Kreuzberg auch in den Ordnungsämtern der Berliner Bezirke die bisher proprietären Insellösungen für Ordnungswidrigkeiten, die nicht mit dem Verkehr zusammenhängen, durch ein einheitliches Verfahren abgelöst werden. Für das neue Verfahren *NOWI* (Nichtverkehrs-Ordnungswidrigkeiten) wurde die Softwarelösung EurOwiG eines bayerischen Softwarehauses gewählt. Das Verfahren ermöglicht den Mitarbeitern der bezirklichen Ordnungsämter, Ordnungswidrigkeiten elektronisch aufzunehmen, zu verarbeiten und zentral zu speichern. Im Rahmen der Unterrichtung erhielten wir professionell erstellte Betriebs- und Sicherheitskonzepte. Eine prüfbare inhaltliche Beschreibung des Verfahrens, insbesondere die notwendige Errichtungsanordnung, die eine datenschutzrechtliche Prüfung ermöglichen würde, liegt allerdings noch nicht vor, obwohl wir Hinweise darauf haben, dass sich das Verfahren bereits im Echteinsatz befindet.

Aus technischer Sicht ist festzustellen, dass das Verfahren in einem sog. Terminalserver-Betrieb arbeitet, bei dem die Mitarbeiter der Ordnungsämter von ihren Arbeitsplatzrechnern über Citrix-Terminalverbindungen mit dem Zentralsystem im ITDZ arbeiten können. Zu solchen Server Based Computing-Architekturen haben wir weiter unten Näheres ausgeführt.[26]

Im Bereich der Stadtentwicklung wurden diverse neue Verfahren aufgesetzt. Das Verfahren zur Verfolgung der Fördermaßnahmen im Wohnumfeldbereich (*WUM*) und das *Korruptionsregister* werden im Berichtsteil „Wohnen und Umwelt“[27] näher behandelt. Auch für die Erteilung von *Baugenehmigungen* wurde ein neues Verfahren europaweit ausgeschrieben. Hier geht es ebenfalls darum, bezirkliche Insellösungen durch ein einheitliches Verfahren zu ersetzen. Jüngst wurden wir auch über das geplante IT-Projekt zur *Erhebung von Straßenausbau- und Erschließungsbeiträgen* unterrichtet.

Der seit Jahren zu beobachtende Trend zu Managementverfahren zur Steuerung (Controlling) und Analyse von Verwaltungsentscheidungen und -verfahren findet seine Fortsetzung im Einsatz des IT-Verfahrens ADONIS zur Modellierung und Analyse von Geschäftsprozessen. Allen derartigen Verfahren ist ge-

[26] vgl. 2.5
[27] vgl. 5.4.1

mein, dass sie auf den Personenbezug der Einzeldaten verzichten können. Es bedarf daher immer wieder unserer Überzeugungsarbeit, dass dies dann auch tatsächlich geschieht. Näheres wird unter „Personaldatenschutz“ ausgeführt[28].

Als Nachfolgesystem des derzeitigen Sozialhilfeverfahrens BASIS wurde uns das Produkt *Open PROSOZ* von der zuständigen Senatsverwaltung angekündigt. Prüfbare Unterlagen liegen noch nicht vor.

Im Bereich des Strafvollzugs werden die bestehenden Altverfahren modernisiert. Auf der Grundlage von Verfahren, die bereits in Nordrhein-Westfalen erfolgreich genutzt werden, setzen die Justizvollzugsanstalten die Verfahren *BASIS-Web* für die Buchhaltung und Abrechnung im Strafvollzug und *Nexus-Web* für die dortigen Arbeitsverwaltungen ein.

2 Schwerpunkte

2.1 *Kinderschutz* und Datenschutz – kein Gegensatz

Wiederholt haben die Medien in den vergangenen Monaten über erschreckende Fälle vernachlässigter oder misshandelter Kinder berichtet. Damit rückte das Problem der *Kindeswohlgefährdung* in den Blickpunkt des öffentlichen Interesses. Zum Teil zeigten sich krasse Defizite bei der frühzeitigen Erkennung und Abwehr von Gefährdungsrisiken durch die beteiligten Personen und Institutionen. Häufig konzentrierte sich die Berichterstattung in derartigen Fällen auf das vermeintlich zwischen Kinderschutz und Datenschutz bestehende Spannungsfeld. Es wurde der unzutreffende Eindruck vermittelt, wirksame Schutzmaßnahmen zur Vermeidung von Kindeswohlgefährdungen würden durch bestehende Datenschutzvorschriften verhindert, die eine Weitergabe von Informationen untersagten. Sollten in Einzelfällen tatsächlich die zur Abwendung einer Kindeswohlgefährdung erforderlichen Datenübermittlungen unterblieben sein, so ist jedoch eher zu vermuten, dass die Ursachen hierfür woanders zu suchen wären und der Datenschutz entweder missverstanden oder gar als Begründung nur vorgeschoben wird.

Pflege und Erziehung der Kinder sind nach dem Grundgesetz (Art. 6 Abs. 2) „das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft.“ Die Wahrung dieses „Wächteramtes“ obliegt der eigens dafür geschaffenen Kinder- und Jugendhilfe.

Der Gesetzgeber hat im Herbst 2005 das Gesetz zur Weiterentwicklung der *Kinder- und Jugendhilfe*

Grundsätzlich stehen die Regelungen des Sozialdatenschutzes den notwendigen Maßnahmen nicht entgegen. Hierauf ist von der Senatsverwaltung für Bildung, Wissenschaft und Forschung auch in ihren Empfehlungen an die Jugendämter zur Umsetzung des Schutzauftrags nach § 8a SGB VIII bei Kindeswohlgefährdung hingewiesen worden. Allerdings muss klargestellt werden, dass es immer wieder Fälle gibt, in denen ein Spannungsverhältnis zwischen Datenschutz und Kinderschutz besteht, da ansonsten keine Abwägung erforderlich wäre, die der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu Recht verlangt. Der Datenschutz ist ein stets präsentes Element bei der Prüfung weiterer Verfahrensschritte in Kinderschutzfällen. Allerdings wird die Aussage begrüßt, dass auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Ansicht teilt, dass notwendige Datenübermittlungen nicht am Datenschutz scheitern und ein anderes Ergebnis eher auf einem missverstandenen Datenschutz beruhen dürfte. Dies gibt den betroffenen Fachkräften damit mehr "Mut zur Handlung".

[28] vgl. 5.3.3

(Kinder- und Jugendhilfeweiterentwicklungsgesetz – KICK)[29] verabschiedet und die zentrale Vorschrift des § 8 a Sozialgesetzbuch VIII – Kinder- und Jugendhilfe (SGB VIII) eingefügt. Die Vorschrift konkretisiert und formuliert den aus dem staatlichen Wächteramt abgeleiteten Schutzauftrag der Kinder- und Jugendhilfe bei Kindeswohlgefährdungen in der Familie und enthält klare Verhaltensvorgaben für das Jugendamt.

Werden dem *Jugendamt* nach § 8 a Abs. 1 Satz 1 SGB VIII gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so hat es das Gefährdungsrisiko im Zusammenwirken mehrerer Fachkräfte abzuschätzen. Soweit gemäß § 8 a Abs. 4 SGB VIII zur Abwendung der Gefährdung das Tätigwerden anderer Leistungsträger, der Gesundheitshilfe oder der Polizei notwendig ist, hat das Jugendamt zunächst darauf hinzuwirken, dass sich die Personensorge- oder Erziehungsberechtigten an diese Stellen wenden, um deren Hilfe in Anspruch zu nehmen. Ist ein sofortiges Tätigwerden erforderlich und wirken die Personensorgeberechtigten oder die Erziehungsberechtigten nicht mit, so schaltet das Jugendamt die anderen zur Abwendung der Gefährdung zuständigen Stellen selbst ein. Der Gesetzgeber hat dem Jugendamt insofern die Befugnis eingeräumt, die zur Abwendung einer Kindeswohlgefährdung erforderlichen Maßnahmen auch durch Einschaltung weiterer Stellen zu ergreifen.

Allerdings bedeutet dies nicht, dass in Fällen von Kindeswohlgefährdungen die datenschutzrechtlichen Vorschriften im Sinne eines in der Praxis häufig angeführten, jedoch gesetzlich in keiner Weise untermauerten Grundsatzes „Kinderschutz vor Datenschutz“ außer Acht zu lassen sind. Vielmehr sind die in § 8 a SGB VIII eingeräumten Befugnisse des Jugendamtes wiederum vor dem Hintergrund der sozialdatenschutzrechtlichen Vorschriften der §§ 61 ff. SGB VIII zu sehen, die vom Gesetzgeber im Rahmen des KICK ebenfalls überarbeitet und dem § 8 a SGB VIII angepasst worden sind.

So sind die Sozialdaten gemäß § 64 Abs. 2 a SGB VIII vor der Übermittlung an eine Fachkraft, die der verantwortlichen Stelle nicht angehört, zu anonymisieren oder zu pseudonymisieren, soweit die Aufgabenerfüllung dies zulässt. Der Gesetzgeber hat also nicht vorgesehen, dass den Fachkräften, die zur Abschätzung des Gefährdungsrisikos hinzugezogen werden, von vornherein personenbezogene Daten zu übermitteln sind. Vielmehr sind diese grundsätzlich zu anonymisieren bzw. zu pseudonymisieren. Hat das Jugendamt die gesetzliche Befugnis, zur Abwendung der *Kindeswohlgefährdung* weitere Stellen einzuschalten, so kann es erforderlichenfalls auch personenbezogen Sozialdaten übermitteln. Als Voraussetzung nennt das

[29] v. 8. September 2005, BGBl. I, 2729

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Gesetz hierfür, dass deren Übermittlung für die Erfüllung der Zwecke erforderlich ist, für die sie erhoben worden sind. Darüber hinaus ist die Datenweitergabe zulässig, wenn sie für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle, d. h. des Trägers der Jugendhilfe, oder einer gesetzlichen Aufgabe eines anderen Leistungsträgers erforderlich ist, an den die Daten übermittelt werden (§ 64 Abs. 1 SGB VIII i. V. m. § 69 Abs. 1 Nr. 1 SGB X).

Sofern das Kriterium der Erforderlichkeit im Einzelfall erfüllt ist, lassen datenschutzrechtliche Vorschriften eine Datenübermittlung an andere Stellen zu. Bei richtiger Anwendung der bestehenden Regelungen ist es kaum vorstellbar, dass einer notwendigen Datenübermittlung, die zur Abwendung einer Kindeswohlgefährdung unterblieben ist, tatsächlich Datenschutzvorschriften entgegenstanden.

Veranlasst durch die auch in Berlin bekannt gewordenen Fälle von Kindeswohlgefährdungen setzte der Berliner Senat Anfang 2006 eine gemeinsame Arbeitsgruppe „*Netzwerk Kinderschutz*“ der Senatsverwaltungen für Bildung, Jugend und Sport sowie Gesundheit, Soziales und Verbraucherschutz unter Beteiligung von Vertretern u. a. der bezirklichen *Kinder- und Jugendgesundheitsdienste* und Jugendämter ein. Wir haben uns ebenfalls an der Arbeitsgruppe beteiligt, um von vornherein datenschutzrechtliche Erwägungen bei der Entwicklung des Konzeptes einbringen zu können. Mit der Einrichtung der Arbeitsgruppe verfolgte der Senat das Ziel, ein Konzept für ein Netzwerk Kinderschutz zu entwickeln, um auf diese Weise den Kinderschutz in Berlin zu verbessern und risikohafte Entwicklungen frühzeitiger erkennen und schneller handeln zu können. In der Arbeitsgruppe wurden Maßnahmen zur Stärkung des Kinderschutzes entwickelt, um durch Prävention, Früherkennung, Beratung, Krisenintervention und rechtzeitige Hilfegewährung der Vernachlässigung von Kindern und der Gewalt gegen Kinder durch Kindesmisshandlung und -missbrauch entgegenzuwirken[30]. Bei Redaktionsschluss lag dieses Konzept dem Rat der Bürgermeister zur abschließenden Stellungnahme vor.

Vgl. die Stellungnahme zum ersten Absatz von 2.1

Ausgehend von der Annahme, dass Fälle von Kindeswohlgefährdungen häufig wegen bestehender Kooperationsdefizite und unklarer Zuständigkeiten zwischen den beteiligten Behörden nicht rechtzeitig erkannt werden, schlug die Arbeitsgruppe „Netzwerk Kinderschutz“ vor, verbindliche Kooperationsvereinbarungen zwischen den Kinder- und Jugendgesundheitsdiensten sowie den Jugendämtern auf bezirklicher Ebene zu

[30] vgl. Mitteilung – zur Kenntnisnahme – über Konzept für ein Netzwerk Kinderschutz (Kinderschutz verbessern – Gewalt gegen Kinder entgegenwirken) und über Kinderschutz stärken, jeweils Schlussbericht, Abgeordnetenhaus Berlin (Drucksache im Erscheinen).

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

schließen[31]. Durch Kooperationsvereinbarungen können allerdings keine neuen Datenverarbeitungsbefugnisse geschaffen werden können. Vielmehr ist eine Datenverarbeitung auch nach Abschluss einer Kooperationsvereinbarung lediglich in dem gesetzlichen Rahmen zulässig, den das SGB VIII für die Jugendämter und das Gesundheitsdienstegesetz (GDG) für die Kinder- und Jugendgesundheitsdienste vorgeben.

In der Arbeitsgruppe wurde der Text einer zwischen den Kinder- und Jugendgesundheitsdiensten und den Jugendämtern auf Bezirksebene abzuschließenden Musterkooperationsvereinbarung entwickelt[32]. Die *Kooperationsvereinbarung* verfolgt das Ziel eines abgestimmten Handelns zur Vorbeugung und frühzeitigen Wahrnehmung von Auffälligkeiten. Die Aufgabenerfüllung der Kinder- und Jugendgesundheitsdienste und der Jugendämter soll in „kooperativer Zusammenarbeit“ und mit gegenseitiger fachlicher Unterstützung erfolgen. Da eine solche Kooperation der Beteiligten einen Austausch personenbezogener Daten voraussetzt, haben wir uns dafür eingesetzt, dass die hierfür bestehenden rechtlichen Befugnisse Eingang in die Musterkooperationsvereinbarung finden.

In der Vereinbarung wird klargestellt, dass eine Übermittlung personenbezogener Daten durch das Jugendamt an den Kinder- und Jugendgesundheitsdienst ohne Einwilligung der Personensorgeberechtigten nur zulässig ist, wenn es für die Erfüllung des Schutzauftrages bei Kindeswohlgefährdung erforderlich ist (§ 64 Abs. 2 SGB VIII i. V. m. § 69 Abs. 1 Nr. 1 SGB X). Eine Übermittlung ist insbesondere zulässig, wenn ein sofortiges Tätigwerden erforderlich ist, die Personensorge- oder Erziehungsberechtigten nicht mitwirken und das Jugendamt die zur Abwendung der Gefährdung zuständigen Stellen selbst einschaltet (§ 8 a Abs. 4 SGB VIII). Wichtig ist, dass durch die Datenübermittlung nicht der Erfolg einer durch das Jugendamt zu gewährenden Leistung infrage gestellt werden darf.

Da die Mitarbeiter der Kinder- und Jugendgesundheitsdienste, aber auch der Jugendämter besonderen Geheimhaltungs- und Verschwiegenheitspflichten unterliegen, ist es notwendig, dass sie diese Pflichten auch in Kinderschutzfällen beachten. Die Betroffenen vertrauen den Mitarbeitern häufig Geheimnisse gerade deswegen an, weil sie sich auf deren berufsrechtliche Verschwiegenheit verlassen. Insofern sind die Regelungen des Kinder- und Jugendhilfegesetzes zu Ver-

[31] vgl. Mitteilung – zur Kenntnisnahme – Konzept für ein Netzwerk Kinderschutz (Kinderschutz verbessern – Gewalt gegen Kinder entgegenwirken), 2. Zwischenbericht, Abghs.-Drs. 15/5016

[32] Anlage 10 der Mitteilung – zur Kenntnisnahme – über Konzept für ein Netzwerk Kinderschutz (Kinderschutz verbessern – Gewalt gegen Kinder entgegenwirken) und über Kinderschutz stärken, jeweils Schlussbericht, Abgeordnetenhaus Berlin (Drucksache im Erscheinen).

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

schwiegenheitspflichten und Datenschutz geradezu eine Voraussetzung für wirksamen Kinderschutz. Sie schreiben auch vor, eine Abwägung dahingehend vorzunehmen, inwiefern die ausnahmsweise Datenübermittlung an eine andere Stelle zur Abwendung der Kindeswohlgefährdung tatsächlich erforderlich ist. Eine Datenübermittlung ist zulässig, wenn sie aufgrund einer Abwägung notwendig ist, um eine gegenwärtige Gefahr für Leben, Gesundheit und Freiheit oder ein anderes gleichwertiges Rechtsgut eines Kindes oder Jugendlichen abzuwenden und es kein milderes gleich geeignetes Mittel gibt.

Kinderschutzfälle führen in der Praxis immer wieder zu der Frage, welche Datenübermittlungen tatsächlich zulässig sind, ohne andere berufsrechtliche Verschwiegenheitspflichten zu verletzen. Um den betroffenen Mitarbeitern die notwendige Rechtssicherheit geben zu können, haben wir Wert darauf gelegt, die bestehenden gesetzlichen Vorgaben für die Datenverarbeitung in der Musterkooperationsvereinbarung ausdrücklich zu benennen. Auf diese Weise wird dafür Sorge getragen, dass die offenbar häufig bestehende Rechtsunsicherheit über die datenschutzrechtlichen Befugnisse in Kinderschutzfällen beseitigt wird. Jedenfalls bedarf es keiner Änderung des Rechtsrahmens, wie sie vereinzelt gefordert worden ist.

Ohnehin kann der Staat nicht mit letzter Sicherheit verhindern, dass Eltern ihre Kinder verwahrlosen lassen oder misshandeln; unter der Geltung des Grundgesetzes ist eine lückenlose Überwachung des Familienlebens ausgeschlossen.

Das Berliner Konzept für ein „Netzwerk Kinderschutz“ ist grundsätzlich geeignet, durch bessere Kooperation der beteiligten Stellen Vernachlässigungen und Misshandlungen von Kindern frühzeitig zu vermeiden. Die datenschutzrechtlichen Rahmenbedingungen sind hierbei zu beachten. Datenschutzrechtliche Vorschriften stehen einer Übermittlung durch den *Kinder- und Jugendgesundheitsdienst* an das Jugendamt nicht entgegen, wenn eine konkrete Kindeswohlgefährdung nicht anders abwendbar ist. Ebenso sind Datenübermittlungen durch das Jugendamt zur Erfüllung des Schutzauftrages des § 8 a SGB VIII zulässig, wenn sie zur Abwendung einer solchen Gefährdung erforderlich sind. Einer Änderung des Rechtsrahmens bedarf es nicht.

Über die Eignung des Konzeptes für ein "Netzwerk Kinderschutz" besteht zwar Konsens. Allerdings ist es durchaus denkbar, dass sich im Zuge der Umsetzung doch noch punktuell ein Bedarf an rechtlichen Präzisierungen oder Änderungen, ergeben könnte. So erscheint es z.B. bezogen auf Schulen möglicherweise als notwendig, Datenübermittlungen zu erlauben, um diese effizienter in den Kinderschutz einbeziehen zu können, damit dem Schutz des Kindeswohls bereits im Vorfeld konkreter Gefährdungen (schleichender beginnender Verwahrlosung) auch unter Beachtung der Elternrechte Rechnung getragen werden kann.

2.2 Fußball-Weltmeisterschaft 2006

Die Fußball-Weltmeisterschaft 2006 war nicht nur in sportlicher Hinsicht ein voller Erfolg. Die im Vorfeld aus Sicherheitskreisen geäußerten Befürchtungen, dass es Randale und Ausschreitungen nicht nur von gewaltbereiten Fußballanhängern oder terroristische Anschläge geben werde, sind keine Realität geworden. Wir haben die umfangreiche Verarbeitung von Zuschauer- und Bewerberdaten vor und bei der Weltmei-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

sterschaft intensiv überprüft.

Akkreditierung

Einen wesentlichen Bestandteil des Sicherheitskonzepts bildeten die Akkreditierungsverfahren, denen sich alle Beschäftigten von Dienstleistungsunternehmen unterziehen mussten, die Zutritt zu bestimmten, nicht-öffentlichen Bereichen der Stadien erhalten sollten. In vergangenen Jahresberichten[33] hatten wir uns bereits ausführlich zu den Vorbereitungen geäußert. Der Polizeipräsident in Berlin hat 13.571 Anträge auf *Akkreditierung* bearbeitet. Davon sind 245 abgelehnt worden. Etwa die Hälfte der Akkreditierungsanträge betraf Personen ohne gespeicherte Auffälligkeiten. Die Sicherheitsbehörden erteilten sofort eine Unbedenklichkeitsbestätigung. Der Rest wurde von Hand bearbeitet. Wenn die Trefferanzeige allein auf Eintragungen beispielsweise als Zeuge oder Geschädigter oder auf nicht relevanten Bagatelldelikten beruhte, erfolgte trotz Treffer ein positives Votum an den tSPOC[34] als Nachmeldung. Alle übrigen Fälle wurden an den seinerzeit für den Trefferfall zuständigen Bearbeiter zur Einzelfallbeurteilung weitergeleitet. Die Daten der Betroffenen wurden mit den Dateien *POLIKS.*, der internen Staatsschutzdatei, INPOL-Z sowie der *Datei "Gewalttäter Sport"* abgeglichen, um ein möglichst umfassendes Bild des strafrechtlich relevanten Verhaltens des Betroffenen zu erhalten.

Darüber hinausgehend erfolgte ein Abgleich mit der Landesdatei "Sportgewalt". Die Erforderlichkeit dafür konnten wir nicht erkennen. Ferner war der Abgleich mit dieser Datei durch die *Einwilligung* des Betroffenen nicht abgedeckt. Die Schwelle für die Speicherung in der Landesdatei "Sportgewalt" ist gegenüber den im Einwilligungsformular erläuterten Straftäter-/Straftatendateien, den Staatsschutzdateien oder der Datei "Gewalttäter Sport" wesentlich geringer. Bereits ein Platzverweis oder ein Antreffen an bestimmten Orten kann für die Aufnahme in die Landesdatei „Sportgewalt“ ausreichen. Weil es für die Zuverlässigkeitsüberprüfung im Zusammenhang mit der Akkreditierung keine Rechtsgrundlage gibt, muss das Verfahren auf die Einwilligung des Betroffenen gestützt werden. Diese ist unwirksam, wenn sie durch fehlende Aufklärung bewirkt wurde.

Die Einbeziehung der Landesdatei „Sportgewalt“ in den Datenabgleich im Rahmen des Akkreditierungsverfahrens war aus polizeilicher Sicht erforderlich, um einen störungsfreien Verlauf der Veranstaltung zu ermöglichen. Die Datei enthält im Vergleich zu der bundesweit genutzten Datei „Gewalttäter Sport“ zusätzliche Angaben, die für die Zuverlässigkeitsüberprüfung der Antragsteller von Bedeutung waren, so zum Beispiel die Zugehörigkeit zu rechtsextremen Organisationen oder zu gewaltbereiten fußballbezogenen Gruppen („Hooligans“).

Die Auffassung, dass die Nutzung der Datei „Sportgewalt“ wegen fehlender Aufklärung der Antragsteller nicht von deren Einwilligung abgedeckt war, teilt der Senat nicht. Die Datenschutzinformation der FIFA informierte die Betroffenen darüber, dass ihre Daten mit verschiedenen polizeilichen Dateien abgeglichen werden, die für Zwecke der Gefahrenabwehr und der Strafverfolgung geführt werden. Dabei wurde ausdrücklich darauf hingewiesen, dass dies auch Dateien der einzelnen Länder sein können. Die genannten Straftäter- und Straftatendateien, die Staatsschutzdateien und die Datei „Gewalttäter Sport“ wurden lediglich beispielhaft aufgezählt. Aus der Datenschutzinformation geht klar her-

[33] JB 2004, 4.1.1; JB 2005, 4.1.2

[34] technischer Single-Point of Contact

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

vor, dass über diese Dateien hinaus weitere Dateien in den Abgleich einbezogen werden konnten. Dass hier speziell auch Landesdateien in Frage kamen, die zur Gefahrenabwehr und Strafverfolgung im Zusammenhang mit Sportveranstaltungen geführt werden, lag auf der Hand.

Die Einwilligungsklausel enthielt zwar eine Aufklärung; in der praktischen Umsetzung aber wurde über den Umfang der informierten Einwilligung hinaus abgeglichen. Auf die Bedeutung der und die Anforderungen an eine präzise Einwilligungserklärung haben die Datenschutzbeauftragten des Bundes und der Länder frühzeitig hingewiesen. Für den Betroffenen muss nachvollziehbar und verständlich sowie transparent sein, was nach der Einwilligung mit seinen Daten geschieht. Das war hier nicht der Fall.

Bei einem Kontrollbesuch bei dem Polizeipräsidenten in Berlin wählten wir nach dem Zufallsprinzip Personen aus dem Kreis des Akkreditierungsverfahrens aus. Es sollte die Übereinstimmung der Ablehnungsgründe mit den Kriterien der Datenschutzinformationen der *FIFA* sowie denen der gleichlautenden Handlungsanleitung für die Sachbearbeitung des Bundeskriminalamtes geprüft werden[35].

Ausgehend vom Ergebnisrücklauf der Ablehnungen bestanden grundsätzlich keine datenschutzrechtlichen Bedenken. In einem Fall hielten wir die Ablehnung für unverhältnismäßig. Die gespeicherten Daten bildeten keine rechtfertigende Grundlage dafür. Das Interesse des Betroffenen an seinem Arbeitsplatz wurde nicht in ausreichender Weise berücksichtigt.

Der genannte Einzelfall wurde nach dem Hinweis des Berliner Beauftragten für Datenschutz und Informationsfreiheit erneut überprüft. Unter Berücksichtigung der vorliegenden Erkenntnisse über den Antragsteller war die ablehnende Empfehlung des Polizeipräsidenten in Berlin aus Sicht des Senats verhältnismäßig.

Daneben haben wir ungeachtet unserer prinzipiellen rechtlichen Einwände gegen die Beteiligung der Verfassungsschutzbehörde am Akkreditierungsverfahren[36] auch dort geprüft. Insgesamt wurden der Berliner Verfassungsschutzbehörde 58 Datensätze vom Bundesamt für Verfassungsschutz zur Überprüfung zugeleitet. Davon wurde in 56 Fällen die Akkreditierung befürwortet, in zwei Fällen wurde sie abgelehnt. Die beiden Ablehnungen betrafen Angehörige einer gewaltbereiten rechtsextremistischen Bestrebung und waren von der Sache her nicht zu beanstanden. In diesen beiden Fällen werden die Vorgänge - wie auch beim Polizeipräsidenten in Berlin - ein Jahr aufbewahrt. Bei den positiv beschiedenen Fällen waren die Vorgänge drei Monate nach Beendigung der Fußball-Weltmeisterschaft 2006 zu löschen.

Soweit der Berliner Beauftragte für Datenschutz und Informationsfreiheit im Zusammenhang im Akkreditierungsverfahren zur FIFA-WM darauf hinweist, dass beim Verfassungsschutz vorhandene Unterlagen zu den positiv beschiedenen Akkreditierungsfällen nach drei Monaten zu löschen waren, teilt der Senat mit, dass diese Löschungen erfolgt sind.

Die beim Verfassungsschutz und beim Polizeipräsidenten in Berlin in den positiv beschiedenen Fällen gespeicherten Daten sind vollständig und fristgerecht gelöscht worden. Der Polizeipräsident (unter Vorlage der Löschprotokolle) und der Verfassungsschutz haben dies dem Berliner Beauftragten für Datenschutz und Informationsfreiheit bereits mitgeteilt

Wir erhielten auch den Hinweis, dass die im Zusammenhang mit der Durchführung der Fußball-Weltmeisterschaft 2006 eingesetzten Polizei- und Feuerwehrbeamten eine Zuverlässigkeitsüberprüfung

Angesichts der besonderen Gefahrenlage während der Fußball-Weltmeisterschaft 2006 war das bei den eingesetzten Feuerwehrleuten durchgeführte Akkreditierungsverfahren nach Auffassung des Senats rechtlich

[35] JB 2005, 4.1.2
[36] JB 2005, 4.1.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

durchlaufen sollten. Dieser Hinweis erwies sich hinsichtlich der Polizei als unzutreffend; die Polizeibeamten sind sicherheitsüberprüft und erhielten deshalb ohne eine erneute Zuverlässigkeitsüberprüfung die Akkreditierungsausweise. Demgegenüber werden Beschäftigte der Feuerwehr nicht sicherheitsüberprüft, sodass insoweit eine Zuverlässigkeitsüberprüfung erfolgte. Hier sollte die informierte Einwilligung der Feuerwehrleute aufgrund der Datenschutzinformation zur Akkreditierung zur Fußball-Weltmeisterschaft 2006 als Rechtsgrundlage dienen.

Dieses Verfahren war rechtswidrig. Es handelt sich um Beamte, die während der Fußball-Weltmeisterschaft 2006 im Rahmen ihrer ordnungsgemäßen Aufgabenerfüllung für die Sicherheit und Ordnung sowie die Gefahrenabwehr sorgen sollten. Beamte sind zuverlässig. Wären sie es nicht, wären sie aus dem Dienst zu entfernen. Darüber bestand auch im Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Einvernehmen. Dass Polizeibeamte - im Gegensatz zu Beschäftigten der Feuerwehr - einer Sicherheitsüberprüfung unterzogen werden, rechtfertigt es jedenfalls nicht, für die Feuerwehr ein Akkreditierungsverfahren vorzusehen, das kein Ersatz für eine standardisierte Sicherheitsüberprüfung sein soll.

vertretbar. Wie der Berliner Beauftragte für Datenschutz und Informationsfreiheit zutreffend ausführt, werden die Beschäftigten der Berliner Feuerwehr bei ihrer Einstellung in den Dienst des Landes keiner Sicherheitsüberprüfung unterzogen. Bei ihrer Einstellung muss lediglich ein Auszug aus dem Bundeszentralregister vorgelegt werden. Aus diesem Grund hatten sich die Bundesländer im Rahmen des Arbeitskreises V der Ständigen Konferenz der Innenminister und –senatoren im März 2006 darauf verständigt, Feuerwehrleute vor ihrer Akkreditierung anders als Polizeibeamte auf ihre Zuverlässigkeit hin zu überprüfen. Der Antrag auf Akkreditierung wurde dabei nur für diejenigen Beschäftigten gestellt, die sich damit einverstanden erklärten. Rechtsgrundlage für die Zuverlässigkeitsüberprüfung der Feuerwehrbeamten war daher wie in allen anderen Fällen auch die informierte Einwilligung.

Weiterhin prüften wir bei verschiedenen Berliner Unternehmen, die Sammelakkreditierungsanträge beim Organisationskomitee (OK) gestellt hatten. Dabei sollte festgestellt werden, ob bei den betroffenen Mitarbeitern eine Einwilligung in die Datenübermittlung eingeholt und zuvor die ausführlichen Datenschutzinformationen ausgehändigt worden waren. Abgesehen davon, dass wir bei zwei Unternehmen die Kopien von Pässen bzw. Personalausweisen der Beschäftigten bei den Unterlagen vorfanden, wurden dabei keine datenschutzrechtlichen Mängel festgestellt.

Insgesamt haben die Erfahrungen mit dem Akkreditierungsverfahren bei der Fußball-Weltmeisterschaft aber eines gezeigt: Es ist rechtlich äußerst problematisch, einem privaten Unternehmen wie der FIFA die Möglichkeit zu eröffnen, gestützt auf Daten der Sicherheitsbehörden Beschäftigungsverbote zu verhängen. Dieses Verfahren sollte kein Vorbild für künftige Großveranstaltungen wie die Leichtathletik-Weltmeisterschaft 2009 in Berlin sein.

Der Senat hält das bei der Fußball-WM durchgeführte Akkreditierungsverfahren für rechtlich zulässig. Die gemachten Erfahrungen geben nach Ansicht des Senats keinen Anlass, zu einer anderen Einschätzung zu gelangen.

Datenverarbeitung im *Olympiastadion*

Schon im Sommer 2005 hatten wir erste Kontakte mit der für das Berliner Olympiastadion zuständigen Senatsverwaltung für Stadtentwicklung und der Betreibergesellschaft aufgenommen. Wir beabsichtigten, für das elektronische *Zutrittskontrollsystem* des Olympiastadions, bei dem mithilfe personenbezogener *Eintrittskarten* zu den Berliner Spie-len im Rahmen der Fußballweltmeisterschaft elektronische Datenabglei-

che vorbereitet wurden, die daten-schutzrechtlichen Rahmenbedingungen zu prüfen.

Diese Überprüfung war dringend angezeigt, weil mit den personenbezogenen Daten der Zutrittsberechtigten im elektronischen Zutrittskontrollverfahren ein Datenabgleich sämtlicher Besucher mit den Dateien über potenzielle Gewalttäter in Rede stand, um deren Zutritt in das Stadion zu verhindern. Nicht nur die privaten Veranstalter mit den beteiligten Unterorganisationen, sondern auch der Staat hatten die Sicherheit der Zuschauer zu gewährleisten. Zugleich musste aber auch den datenschutzrechtlichen Erfordernissen Rechnung getragen werden, um bei der Personenkontrolle den Missbrauch der personenbezogenen Daten auszuschließen.

Die elektronische Zutrittskontrolle anhand personenbezogener Daten ist mit Recht als bisher einmaliger Vorgang in diesem Maßstab bezeichnet worden. Denn Zehntausende von Personen sollten in kürzester Zeit durch das elektronische Kontrollsystem geschleust werden und bei jedem Besucher sollte die Zugehörigkeit zu einer der gewaltorientierten Gruppierungen wie *Hooligans*, Randalierer und terrorismusverdächtige Szene möglichst ausgeschlossen werden, um die im Stadion versammelten Zuschauer nicht einer Gefahr auszusetzen.

Um einerseits die Möglichkeit eines Datenmissbrauchs auszuschließen und andererseits die Funktionssicherheit des Systems zu gewährleisten, mussten klare datenschutzrechtliche Verantwortlichkeiten definiert werden. Dabei waren auch die räumliche Installation aller elektronischen Anlagen und die lokalen Netze sowie deren Vernetzung nach innen und außen in eine Überprüfung einzubeziehen. Es mussten Sicherheitsstandards erfüllt werden, die die Datenverarbeitung nicht nur vor einem äußeren Angriff schützten, sondern auch einen internen missbräuchlichen Zugriff oder missbräuchliche Verarbeitung zu verhindern hatten.

Nach den vertraglichen Unterlagen, die uns die beteiligten Organisationen zur Verfügung gestellt hatten, war die Betreibergesellschaft (Olympiastadion-Betreibergesellschaft – OSTA-BG) einerseits als Auftragnehmerin des Organisationskomitees Deutschland der FIFA bei der Datenverarbeitung anzusehen und unterlag andererseits den Regelungen des § 11 Bundesdatenschutzgesetz (BDSG). Im Rahmen dieser Vorschrift trug sie eine eigene datenschutzrechtliche Verantwortung. Die Betreibergesellschaft durfte bei der Kontrolle der personenbezogenen Eintrittskarten die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten und nutzen. Das Organisationskomitee Deutschland unterlag als Auftraggeber den gesetzlichen Bestimmungen des § 11 Abs. 1 und § 28 BDSG. Es hatte das Organisationsrecht und die Pflicht, auf die Wahrung des Datenschutzes hinzu-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

wirken. Die Betreibergesellschaft konnte jedoch nicht aus einer eigenen datenschutzrechtlichen Verantwortung entlassen werden, zumal sie nach dem Vertragstext ausdrücklich für eine funktionierende Technik und damit auch für die eingesetzte Datenverarbeitungstechnik verantwortlich war. Die Vereinbarung, dass die Betreibergesellschaft keinerlei eigene Zugriffsmöglichkeiten oder Rechte an den Daten der Zuschauer haben sollte und sie auch nicht auf die Verarbeitung personenbezogener Daten einwirken durfte, war allerdings als strikte Weisung des Organisationskomitees Deutschland der FIFA an die Betreibergesellschaft zu sehen, keinen Zugriff auf personenbezogene Daten zu nehmen. Dies schmälerte jedoch nicht die in § 11 Abs. 4 BDSG zum Ausdruck gekommene eigene datenschutzrechtliche Verantwortung und Verhaltens- und Organisationspflicht. Deshalb war die Betreibergesellschaft als Auftragnehmerin für die Umsetzung der technisch-organisatorischen Maßnahmen nach § 9 BDSG mitverantwortlich.

Vor diesem rechtlichen Hintergrund haben wir bei der Betreibergesellschaft das elektronische Zutrittssystem überprüft. Wir haben unsere datenschutzrechtlichen Maßnahmen mit dem Regierungspräsidium Darmstadt, das die zuständige Aufsichtsbehörde nach dem Bundesdatenschutzgesetz für das Organisationskomitee Deutschland war, abgestimmt.

Auch wenn beim Zutrittskontrollverfahren in Berlin keine gravierenden datenschutzrechtlichen Mängel festgestellt wurden, wecken Medienberichte aus anderen Austragungsorten erhebliche Zweifel an der Verhältnismäßigkeit des flächendeckenden Einsatzes personalisierter Eintrittskarten. So wurden offenbar beim Eröffnungsspiel in München allenfalls stichprobenhafte Kontrollen durchgeführt. Nach Angaben der FIFA war dies bei allen Spielen nie anders geplant.

Im Bundesliga-Alltag sollten RFID-bestückte Eintrittskarten zur Identifizierung der Zuschauer jedenfalls keine Schule machen.

Unabhängig von den nur eingeschränkten Möglichkeiten der Einflussnahme auf die vertraglichen Regelungen bei der Bewerbung Berlins um sportliche Großveranstaltungen wird sich der Senat bemühen, bei künftigen Veranstaltungen auf datenschutzrechtlich einwandfreie Verfahrensweisen des Veranstalters hinzuwirken.

Videoüberwachung

Gegenstand unserer Überprüfung war auch die Videoüberwachung am und im Olympiastadion Berlin, für die während der Fußball-Weltmeisterschaft 2006 der Polizeipräsident in Berlin verantwortliche Stelle war. Als Rechtsgrundlage konnte er sich dabei auf § 24 Abs. 1 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) stützen. Danach kann die Polizei bei oder im Zusammenhang mit öffentlichen, nicht dem Versammlungsgesetz unterliegenden Veranstaltungen oder Ansammlungen personenbezogene Daten durch Ermittlungen oder durch den Einsatz technischer Mit-

tel zur Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmern erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Dabei dürfen auch personenbezogene Daten über Dritte erhoben werden, soweit das unvermeidbar ist, um eine Datenerhebung durchführen zu können. Verdeckte Bild- und Tonaufzeichnungen sind unzulässig.

Für die Fußball-Weltmeisterschaft 2006 wurde die bisherige Videoüberwachung rund um das Olympiastadion Berlin ausgeweitet, um den Besucherstrom an den Spieltagen besser überwachen und lenken zu können. Die Kamerabilder liefen in der Leitzentrale des Olympiastadions Berlin zusammen, von wo aus sämtliche Sicherheitskräfte aufgrund der Auswertung der Bildinformationen dirigiert werden konnten. Die Aufzeichnungen wurden ausschließlich von einem Stab speziell geschulter und zugangsberechtigter Mitarbeiter der verantwortlichen Stelle erstellt und ausgewertet. Die Kameras waren nicht verdeckt installiert.

Zur Sicherung der *Fanmeile* auf der Straße des 17. Juni und am Brandenburger Tor wurden zehn Videokameras eingesetzt, um etwaige Unruhestifter vor und auf dem Veranstaltungsgelände frühzeitig erkennen zu können. Auch sollten damit die Besucherströme gelenkt werden. Verantwortliche Stelle war hier die Senatskanzlei als Vertreter des Landes Berlin, dem das Veranstaltungsgelände gehört. Die Senatskanzlei kooperierte sehr eng mit der Polizei. Diese hatte damit auch weitgehend Zugriff auf die Videodaten. Die Senatskanzlei berief sich bei ihrem Vorgehen auf das Berliner Datenschutzgesetz und insbesondere auf das Hausrecht des Landes Berlin im umzäunten Bereich der Fanmeile. Dies rechtfertigt aber nicht, die polizeirechtlichen Voraussetzungen einer Videoüberwachung zu relativieren.

Für künftige Großveranstaltungen sollte hinsichtlich der Videoüberwachung und der Bildaufzeichnungen folgende Rechtslage beachtet werden: Sofern Tatsachen die Annahme rechtfertigen, dass bei oder im Zusammenhang mit öffentlichen, nicht dem Versammlungsgesetz unterliegenden Veranstaltungen oder Ansammlungen Straftaten begangen werden, kann die Polizei nach § 24 ASOG personenbezogene Daten durch Ermittlungen oder den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmern erheben. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die Maßnahme nur eingesetzt wird, wenn ohne sie die Erfüllung des verfolgten Zweckes nicht möglich wäre oder zumindest erheblich erschwert würde. Nach den Vorstellungen des Gesetzgebers soll die Gesamtmaßnahme durch die Erfassung polizeilich nicht relevanter Dritter nicht infrage gestellt werden. Gezielte Aufnahmen und die gezielte Aufzeichnung solcher Dritter (z. B. durch digitale Bildmarkierungen zur Ermöglichung von gezieltem Suchen in Aufzeichnungsbeständen) sind al-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

lerdings regelmäßig nicht erlaubt.

Aufgrund der polizeirechtlichen Sonderregelung im ASOG konnte sich die Polizei nicht auf § 31 b Berliner Datenschutzgesetz (BlnDSG) als Befugnisnorm für die Videoüberwachung stützen. Da hier die Senatskanzlei als Veranstalter auftrat, war nur für sie § 31 b BlnDSG heranzuziehen. Entsprechendes gilt für Videoüberwachung zur Wahrung des Hausrechtes der verantwortlichen Stelle. Die drohende Begehung einer Straftat ist also – anders als im Polizeirecht - nicht Voraussetzung für die Zulässigkeit der Beobachtung.

Eine Bildaufzeichnung darf erfolgen, wenn sie "zum Erreichen des verfolgten Zweckes erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen Bilder nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist." Die Voraussetzungen für die Zulässigkeit der Videoüberwachung sind im Berliner Datenschutzgesetz teilweise geringer, teilweise abweichend vom Polizeirecht geregelt. Somit könnte die Polizei bei dem Zugriff auf die nach § 31 b BlnDSG aufgezeichneten Videodaten ihr Datenzugriffsspektrum erweitern. Das aber lässt das Polizeirecht nicht zu.

Für den Zugriff auf Bild- und Tonaufzeichnungen anderer öffentlicher oder nicht-öffentlicher Stellen braucht die Polizei eine bereichsspezifische Erhebungsgrundlage. Verlangt sie diesen zu präventiven Zwecken, kann sie sich dabei nicht auf die Generalklausel zur polizeilichen Datenerhebung stützen (§ 18 Abs. 1 ASOG). Denn diese Vorschrift weist deutlich niedrigere Eingriffsschwellen auf als die Befugnis zur polizeieigenen offenen Bild- und Tonaufzeichnung. Um eine Umgehung der vom Berliner Gesetzgeber festgelegten Eingriffsschwellen zu vermeiden, ist deshalb eine bereichsspezifische Rechtsgrundlage zu schaffen, die bisher fehlt.

Da private Veranstalter bereits im Planungsstadium häufig die Auflage zur Videoüberwachung erhalten, könnte man von dem beschriebenen Erfordernis einer bereichsspezifischen Erhebungsgrundlage allenfalls unter der Bedingung absehen, dass der Zugriff auf private Aufzeichnungen nur unter solchen Bedingungen erfolgen darf, unter denen auch eine polizeiliche Aufzeichnung möglich wäre. Gleichzeitig darf die verantwortliche nicht-öffentliche Stelle einen Zugang nur dann gestatten, wenn die Zulässigkeitsvoraussetzungen des § 24 ASOG und des für privaten Veranstalter geltenden § 6 b BDSG kumulativ erfüllt sind. Der Zugriff auf Bild- und Tonmaterial zu Zwecken der Beweissicherung im Rahmen der Strafverfolgung kann nur unter den Voraussetzungen der Beschlagnahme erfolgen (§§ 94, 98 StPO). Für die nicht-öffentlichen Stellen stellt die Übergabe der Bild- und Tondaten

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

eine Zweckänderung gegenüber dem ursprünglichen Erhebungszweck dar. Diese Zweckänderung kann bereits nach § 6 b BDSG zulässig sein, findet aber ihre Rechtsgrundlage jedenfalls in dem rechtmäßigen Herausgabeverlangen der Polizei.

Sofern auch künftig zur Sicherung von Großveranstaltungen öffentliche oder private Veranstalter Videoaufzeichnungen vornehmen und der Polizei der Zugriff darauf gestattet werden soll, sind hierfür die rechtlichen Voraussetzungen zu schaffen. Im Rahmen dieses Gesetzgebungsvorhabens sollten die hier beschriebenen Standards nicht unterschritten werden.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit stellt die Rechtslage zutreffend dar. Eine polizeiliche Nutzung der durch den Veranstalter erhobenen Videodaten auf der Fanmeile erfolgte nur in dem vorgegebenen rechtlichen Rahmen:

Soweit die Polizei die Bildaufzeichnungen des Veranstalters (mit-)nutzte, tat sie dies, da die Voraussetzungen des § 24 Absatz 1 ASOG vorlagen, sie also die Daten auch selbst hätte erheben dürfen. Der Übertragungsraum des Veranstalters der Fanmeile war nur dann mit Mitarbeitern der Polizei besetzt, wenn dies aufgrund der jeweiligen Lagebewertung und der daraus folgenden Gefahrenprognose erforderlich schien. Die Gefahrenprognosen beruhten auf zuvor erlangten konkreten Hinweisen auf geplante Störungen durch Hooligans sowie auf vorangegangenen Vorkommnissen (sog. „Drittortauseinandersetzungen“) und anderen aktuellen Erkenntnissen, die eine Begehung von Straftaen vermuten ließen.

Anzumerken ist im Übrigen, dass der Berliner Beauftragte für Datenschutz und Informationsfreiheit während der Fußball-WM gemeinsam mit der Senatskanzlei den Videoüberwachungscontainer auf der Fanmeile besichtigte und dabei keine Bedenken oder Beanstandungen äußerte.

Daher besteht nach Auffassung des Senats kein Anlass für die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit implizierte Unterstellung, die Seatskanzlei und / oder der Polizeipräsident in Berlin hätten die rechtlichen Voraussetzungen einer Videoüberwachung relativiert.

Der Senat teilt die Auffassung, dass im Interesse der Rechtssicherheit eine bereichsspezifische Rechtsgrundlage für die polizeiliche Nutzung von Bildaufzeichnungen bei öffentlichen Veranstaltungen geschaffen werden sollte. Eine entsprechende Ergänzung des § 24 ASOG wird derzeit vorbereitet.

2.3 Die *Warndatei* der Versicherungswirtschfat – eine Blackbox

„Ich willige ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/Versicherungsveränderungen) ergeben, zur Beurteilung des Risikos und der Ansprüche an andere Versicherungen und/oder an den Gesamtverband der Deutschen Versicherungswirtschaft zur Weitergabe dieser Daten an andere Versicherer übermittelt.“

Kaum ein Versicherungsnehmer, der bei Vertragsabschluss diese einheitliche *Einwilligung*serklärung der Versicherungswirtschaft unterschreibt, wird sich über die Folgen seiner Unterschrift für sein informationelles Selbstbestimmungsrecht im Klaren sein. Kein Versicherungsnehmer hat die vom Bundesverfassungsgericht[37] geforderte Möglichkeit zum „*informationellen Selbstschutz*“. Die Abgabe der Einwilligungserklärung ist „freiwillig“, wer sich allerdings weigert, sie abzugeben, erhält keinen Versicherungsvertrag. Da alle Unternehmen der Versicherungswirtschaft mit dieser Einwilligungserklärung arbeiten und keine Versicherung bereit ist, ohne ihre Abgabe einen Versicherungsvertrag abzuschließen, verstößt die Praxis der Versicherungswirtschaft gegen § 4 a Abs. 1 Satz 1 BDSG. Danach ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.

Das *Hinweis- und Informationssystem* der Versicherungswirtschaft wird in den Sparten Leben, Unfall, Kraftfahrt, Rechts-schutz, Sachversicherungen, Transport und Haftpflicht geführt. Die Datei soll die Versicherungsbranche nicht nur vor Versicherungsbetrügern bei Vertragsabschluss und Schadensregulierung warnen, sondern auch vor Versicherungsnehmern, bei denen ein erhöhtes Risiko besteht, dass ein Versicherungsfall eintreten könnte. Gegenüber diesem Personenkreis wird ein Vertragsabschluss entweder abgelehnt oder es werden erhöhte Prämien verlangt. Dies gilt etwa für Rechtsschutzversicherte, die mehrmals ihre Rechtsschutzversicherung in Anspruch genommen haben.

In der Warndatei werden nicht nur die Daten Versicherter gespeichert, sondern auch von Versicherungsantragstellern, deren Versicherungsvertrag nicht zustande gekommen ist, und Dritten, wie etwa der Geschädigte in einem Haftpflichtfall oder der Zeuge des Schadensfalles.

Für jede einzelne Sparte sind Einmeldekriterien entwickelt worden (Gebot der Spartentrennung). Die einzelnen Kriterien und die jeweilige Gewichtung der Kriterien werden von der Versicherungswirtschaft gegenüber den Versicherungsnehmern geheim gehalten, für diese ist somit nicht erkennbar, ob sie in die schwarze Liste der Versicherungswirtschaft aufgenommen wurden.

Bei der Mehrzahl der Sparten-Systeme ist eine Meldung nur dann vorzunehmen, wenn nach dem Kriterienkatalog die Punktzahl 60 erreicht wird. Falls diese Punktzahl erreicht wird, haben die Sachbearbeiter in den Versicherungen die Verpflichtung, eine Einmeldung vorzunehmen. Den hierzu erstellten „Compli-

[37] Beschluss v. 23. Oktober 2006 – 1 BvR 2027/02

ance-Regelungen“ ist nicht zu entnehmen, dass etwa auf eine Meldung verzichtet werden kann, wenn trotz des Erreichens einer bestimmten Punktzahl sicher davon ausgegangen werden kann, dass keine Unregelmäßigkeit vorliegt.

Bei der Entwicklung der Kriterien wurde kein wissenschaftlich-statistischer Ansatz gewählt. Bei der Betrugsprävention etwa in der Sparte Kraftfahrt, aber auch in anderen Sparten, wurden die Kriterien nach Angaben der Versicherungswirtschaft unter Auswertung der Rechtsprechung der Oberlandesgerichte und des Bundesgerichtshofes entwickelt. Auch die Punktzahl richte sich nach der Rechtsprechung. Bedenkt man, dass sich die Rechtsprechung mit Einzelfällen befasst, erscheint es als nicht unproblematisch, dass Indizien, die in einem Einzelfall den Ausschlag für die Beweiswürdigung gaben, anschließend „als Auswertung der Rechtsprechung“ pauschal in Warnsystemen verwendet werden. Wie die Auswertung der Rechtsprechung zu bestimmten Punktzahlen führt, ist völlig unklar.

Bei einer Analyse der den Aufsichtsbehörden ausgehändigten Kriterien stellt man fest, dass die Mehrzahl der K.-o.-Kriterien (60 Punkte) als plausibel erscheint. Allerdings eröffnen viele *Einmeldekriterien* dem Rechtsanwender beträchtliche Ermessensspielräume, teilweise ist juristischer Sachverstand vonnöten, wenn etwa ein subjektiver Tatbestand bewertet werden muss. Hier ist absehbar, dass die einmeldenden Sachbearbeiter überfordert sind und es wenig wahrscheinlich ist, dass die einzelnen Kriterien gleichmäßig ausgelegt werden. Wenn ein Kriterium an ein Gerichtsverfahren anknüpft, ist nicht erkennbar, wie die Versicherungswirtschaft sicherstellt, dass ein später erfolgter Freispruch in der schwarzen Liste berücksichtigt wird.

Die Versicherungssachbearbeiter verfügen bei jeder Sparte über ein Einmeldeformular. Die ausgefüllten Formulare werden an den Gesamtverband der Versicherungswirtschaft (GDV) weitergeleitet. Dieser verarbeitet die personenbezogenen Daten, die das Einmeldeformular enthält, in Auftragsdatenverarbeitung (§ 11 BDSG). Der GDV verarbeitet die personenbezogenen Daten mithilfe einer Software, der sog. *Uniwagnis* 1. Aus Nachnamen, Vornamen und Adresse des Betroffenen wird mithilfe der Software ein phonetischer Buchstabencode erstellt, dieser wird anschließend in einen Zahlencode umgewandelt; am Ende des Prozesses verfügt der GDV nur noch über einen Zahlencode. Die Klarsichtdaten werden noch eine Zeit lang zur Sicherung auf besonders geschützten Datenträgern bei einem Notar aufbewahrt. Der GDV hat keine Möglichkeit, den Zahlencode zu dechiffrieren, da ihm hierfür die erforderliche Software, Uniwagnis 2, fehlt.

Diese Auffassung ist nicht nachvollziehbar. Die Un-

klarheiten, die aufgrund der phonetischen Codierung bestehen, entsprechen etwa denen, die bestehen, wenn man einen mit lateinischen Buchstaben geschriebenen Namen ins Hebräische überträgt und anschließend wieder zurückübertragen möchte. Auch hier bestehen aufgrund der im hebräischen üblichen Auslassungen Unsicherheiten, trotzdem wird man hebräisch geschriebene Namen nicht als anonymisiert ansehen können.

Das Hauptproblem besteht allerdings darin, dass der Versicherungssachbearbeiter bei einem Versicherungsantrag über sehr viele Informationen verfügt. Selbst wenn ein Stefan Meier (mit welcher Schreibweise auch immer) in einem Hochhaus in Berlin wohnt, ist die Wahrscheinlichkeit nicht sehr groß, dass es in diesem Haus einen zweiten Stefan Meier mit gleichem Geburtsdatum gibt. Bei weniger geläufigen Namen mit weniger Schreibvarianten ist die Treffersicherheit noch größer, insbesondere dann, wenn der Betroffene nicht in einem Hochhaus, sondern in einem Ein- bis Dreifamilienhaus wohnt.

Die Informationen, die das Hinweissystem nach der Dechiffrierung durch Uniwagnis 2 enthält, reichen also aus, um bei einem Antrag ohne Anruf bei der einmeldenden Versicherung festzustellen, dass es zu einer bestimmten Person mit an Sicherheit grenzender Wahrscheinlichkeit einen Eintrag gibt. Nur wenn der Versicherungssachbearbeiter weitere Informationen zu dem Vorfall wünscht, ist er gezwungen, diese über einen zusätzlichen Anruf bei der einmeldenden Versicherung zu erhalten. Es besteht auch die Möglichkeit, über Bekannte und Verwandte, die keinen Versicherungsantrag gestellt haben, deren Anfragedaten jedoch bekannt sind, festzustellen, ob ein Hinweis in der Warndatei vorliegt. Wenn es zu einem Telefongespräch zwischen den Sachbearbeitern der abfragenden und der einmeldenden Versicherungen kommt, ist nicht sichergestellt, dass sich die Information auf die für den Abfragenden erforderlichen Daten beschränkt.

Entgegen den Vorgaben des § 33 BDSG wird der Betroffene über die Einmeldung in diese *schwarze Lite* nicht informiert. Hierüber wird der Betroffene – wenn überhaupt – erst Informationen erhalten, wenn er aufgrund der Einmeldung einen Versicherungsvertrag nicht oder zu ungünstigen Konditionen erhält oder sich eine Schadensregulierung verzögert. Auch hier ist nicht sichergestellt, dass die Versicherung, mit der er Verhandlungen führt, ihn ausreichend über die Gründe für die o. g. Konsequenzen informiert. Erhält er nur den Hinweis auf das Vorhandensein der Hinweissysteme, ist für ihn, falls er häufiger die Versicherung gewechselt hat, auch nicht transparent, wer die Einmeldung vorgenommen hat. Falls es dem Betroffenen gelingt, die einmeldende Stelle zu identifizieren, wird er auch nur in einem sehr beschränkten Ausmaß Informationen erhalten, da die einzelnen Kriterien der Hinweis- und Warnsysteme als *Betriebsgeheimnis* angese-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

hen werden. Die mangelnde Transparenz führt auch dazu, dass der Betroffene nicht die Möglichkeit hat, in ausreichendem Maße Ansprüche auf Berichtigung nach § 35 BDSG durchzusetzen.

Es ist nicht möglich, das zurzeit von der Versicherungswirtschaft verwendete Hinweis- und Informationssystem durch kleinere Strukturveränderungen und durch eine Verbesserung der Transparenz datenschutztauglich zu gestalten. Der Versicherungswirtschaft ist deshalb zu empfehlen, ihr teilweise berechtigtes Informationsinteresse durch den Aufbau einer branchenspezifischen Auskunftei sicherzustellen. Dies hätte den Vorteil, dass Datenübermittlungen an diese Datei sich nicht an einer zweifelhaften Einwilligungserklärung, sondern an den Vorgaben des § 29 BDSG orientieren müssten. Danach dürften keine „weichen Daten“ eingemeldet werden. Die Warnmeldungen würden nicht allen Versicherungen zur Verfügung gestellt (Vorratsdatenspeicherung), diese müssten vielmehr das Vorliegen eines berechtigten Interesses nachweisen. Auch eine gewisse Transparenz wäre sichergestellt, der Betroffene müsste über die erstmalige Übermittlung durch die Auskunftei informiert werden (vgl. § 33 BDSG). Die Auskunft über die gespeicherten Daten dürfte nur unter den engen Voraussetzungen des § 34 Abs. 4 i. V. m. § 33 Abs. 2 Nr. 2, 3 und 5 bis 7 BDSG verweigert werden.

Das *Hinweis- und Informationssystem* der Versicherungswirtschaft verstößt gegen das Bundesdatenschutzgesetz und sollte durch ein datenschutzkonformes Auskunfteisystem ersetzt werden.

2.4 Gesundheitliche *Prävention* und Eingliederungsmanagement

Grundsätze und Ziele des *Eingliederungsmanagements*

Die Präventionsvorschrift des § 84 Abs. 2 Sozialgesetzbuch IX (SGB IX) verpflichtet alle privaten und öffentlichen Arbeitgeber zum Eingliederungsmanagement, sobald ein Arbeitnehmer länger als sechs Wochen ununterbrochen oder wiederholt innerhalb eines Jahres (nicht Kalenderjahr) arbeitsunfähig ist. Das betriebliche und behördliche Eingliederungsmanagement, das zur Fürsorgepflicht des Arbeitgebers für erkrankte Mitarbeiter gehört, ist dabei nicht nur für Behinderte und Schwerbehinderte, sondern für sämtliche Beschäftigte und unabhängig von der Betriebs- oder Dienststellengröße durchzuführen. Auch wenn das Sozialgesetzbuch Regelungsort des Eingliederungsmanagements ist, stellen die für den jeweiligen Betrieb zu erhebenden Daten keine Sozialdaten im Sinne des Sozialgesetzbuches dar. Die Bewertung datenschutzrechtlicher Problemstellungen richtet sich daher nach den Datenschutzgesetzen des Bundes und der Länder.

Der Senat begrüßt die ausführlichen Erläuterungen und Hinweise zu diesem wichtigen Komplex. Die von der Senatsverwaltung für Inneres und Sport mit dem Hauptpersonalrat gegenwärtig entwickelte "Dienstvereinbarung Gesundheit" (DV Ges) widmet dem Betrieblichen Eingliederungsmanagement (BEM) einen eigenen Abschnitt und folgt damit und darin den Anregungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Der aktuelle Bericht führte auch dazu, die bisherigen Formulierungen mit Blick auf die landesweite einheitliche Anwendung noch schärfer und eindeutiger zu fassen. Dies betrifft u.a. auch den Hinweis des Berliner Beauftragten für Datenschutz und Informationsfreiheit, dass es sich bei den zu erhebenden Daten nicht um Sozialdaten im Sinne des SGB handelt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Das Eingliederungsmanagement dient der möglichst frühzeitigen Erkennung von gesundheitlichen Problemen der Beschäftigten. Es soll die Gesundheit der Belegschaft schützen, erhalten oder schnellstmöglich wieder herstellen. Sinn und Zweck dieser Regelung ist es, umgehend zu klären, wie die Arbeitsunfähigkeit überwunden, Fehlzeiten verringert und mit welchen Hilfen und Leistungen einer erneuten Arbeitsunfähigkeit vorgebeugt werden kann. Ziel dabei ist, rechtzeitig einer Gefährdung des Arbeitsplatzes aus gesundheitlichen Gründen entgegenwirken zu können.

Die Regelung verschafft damit der Gesundheitsprävention am Arbeitsplatz einen stärkeren Stellenwert als bisher, weil die Beteiligten, besonders der Arbeitgeber, zum zügigen Handeln verpflichtet werden. Das Eingliederungsmanagement erfordert damit unabhängig von konkreten Fehlzeiten:

- Instrumente zur Erfassung und Spezifizierung der gesundheitlichen Probleme, wie z. B. Ergebnisse aus Mitarbeiterbefragungen oder Fehlzeitenerfassung,
- eine Schaltstelle für die Verarbeitung, Entscheidung und Umsetzung (Integrationsteam) sowie
- eine Dokumentation zur Evaluierung.

Bereits daraus wird deutlich, dass zahlreiche Fragen des Arbeitnehmer- und Personaldatenschutzes entstehen.

Der Gesetzgeber hat in § 84 Abs. 2 Satz 1 SGB IX festgelegt, dass der Betroffene sein Einverständnis geben muss, damit ein Eingliederungsmanagement durchgeführt werden kann. Damit beruht das Eingliederungsmanagement auf den Prinzipien der Freiwilligkeit und des Dialoges. Entscheidend für eine erfolgreiche Durchführung des Eingliederungsmanagements ist vornehmlich, den Betroffenen die Angst vor der Mitwirkung im Eingliederungsmanagement zu nehmen. Daher setzt das Eingliederungsmanagement strikte Verschwiegenheit gegenüber Dritten sowie Transparenz und Sensibilität gegenüber dem Betroffenen voraus. Als Beteiligte im Integrations-/Eingliederungsteam nennt der Gesetzgeber den Betroffenen, einen Vertreter der Dienststelle sowie die Personalvertretung. Darüber hinaus sind jedoch ggf. auch die Frauenvertretung und die Schwerbehindertenvertretung zu beteiligen. Sowohl der Betroffene als auch die Schwerbehindertenvertretung können die Durchführung des Eingliederungsmanagements gerichtlich durchsetzen. Auf besonderen Wunsch des Betroffenen können zudem ein Arzt oder eine Person seines Vertrauens sowie Fachkräfte (Arbeitssicherheit, Sucht, Prävention) hinzugezogen werden. Der Betroffene ist auch berechtigt, einzelne Personen des Eingliederungsteams von der Teilnahme auszuschließen und andere hinzuzuziehen.

Die Beschreibung der Voraussetzungen und die Auswahl der Akteure findet sich ebenfalls in dem Entwurf der DV Ges wieder, hier noch ergänzt um das tragende Verfahrensprinzip "Konsens". So sind in den Dienststellen Integrationsteams zu bilden, die für eine einheitliche und fachkompetente Umsetzung des Verfahrens sorgen sollen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Verfahren zum Eingliederungsmanagement

Liegen die Voraussetzungen zur Durchführung eines Eingliederungsmanagements (sechswöchige Krankheit innerhalb eines Jahres (nicht Kalenderjahr)) vor, sollte der Arbeitgeber mit dem Betroffenen schriftlichen oder mündlichen Kontakt zur Durchführung des Eingliederungsmanagements aufnehmen. Die Personalvertretung ist über diese Kontaktaufnahme zu informieren. In diesem Gespräch oder Schreiben sollte dem Betroffenen die Wahlmöglichkeit der am *Integrationsteam* beteiligten Personen gegeben werden. Ist der Betroffene mit der Durchführung des Eingliederungsmanagements nicht einverstanden, so sind sämtliche diesbezügliche Aktivitäten einzustellen und die Personalstelle zu unterrichten. Erteilt dagegen der Betroffene sein Einverständnis zur Durchführung des Eingliederungsmanagements, sollte das Integrationsteam unverzüglich mit dem Betroffenen das gewünschte Gespräch führen.

Gesprächsvermerke, Protokolle oder Vereinbarungen sollten dabei von dem Gesprächsführer und dem Betroffenen unterzeichnet und dem Betroffenen in Kopie ausgehändigt werden. Im Übrigen verbleiben sie in der Dienststelle bzw. beim Gesprächsführer. Da es sich bei den in den Unterlagen enthaltenen Daten um sensitive Daten im Sinne des § 3 Abs. 9 Bundesdatenschutzgesetz handelt, ist über deren Inhalt strengste Verschwiegenheit zu wahren. Sie sind vor dem Zugriff Dritter zu schützen und nicht länger als fünf Jahre aufzubewahren. Wenn die festgelegte Maßnahme zum Erfolg geführt hat, ist das Eingliederungsmanagement beendet. Dasselbe gilt, wenn der Betroffene unabhängig von der Verfahrensstufe dies wünscht. Das Eingliederungsmanagement ist auch dann beendet, wenn in einem weiteren Gespräch festgestellt wird, dass weitere Maßnahmen nicht möglich bzw. nicht erfolgversprechend sind. Sämtliche Unterlagen sind in diesen Fällen unverzüglich zu vernichten und die Personalstelle von der Beendigung zu unterrichten.

Wünscht der Betroffene die Beendigung des Eingliederungsmanagements, so dürfen ihm daraus keinesfalls Nachteile erwachsen.

Die Vereinheitlichung über die reinen gesetzlichen Vorgaben hinaus soll neben den grundsätzlichen Ausführungen zur Rahmengestaltung in der DV Ges insbesondere durch praktische Handlungshilfen gesichert werden. Diese Unterlage wird allen Dienststellen von der Zentralen Stelle für Gesundheitsmanagement bei der Senatsverwaltung für Inneres und Sport zur Verfügung gestellt werden.

Die Handlungshilfe beinhaltet u.a.
- Beteiligte Personen
- Schritte des BEM
- Musterblätter
  z.B. Anschreiben an Dienstkräfte, Dokumentation etc.

In die Handlungshilfe werden ebenfalls weitere detaillierte Hinweise aus dem Jahresbericht des Berliner Beauftragte für Datenschutz und Informationsfreiheit einfließen.

Verstöße gegen § 84 Abs. 2 SGB IX und deren Rechtsfolgen

Sanktionen für den Arbeitgeber, der seiner Pflicht nach § 84 Abs. 2 SGB IX nicht nachkommt, sieht diese Vorschrift an keiner Stelle vor. Der Verstoß gegen die Regelung stellt auch keine Ordnungswidrigkeit im Sinne des § 156 SGB IX dar, da die dortige Aufzählung wohl abschließend ist. Nach einer Entscheidung des Landesarbeitsgerichts Berlin[38] ist

In der Handlungshilfe wird diesbezüglich für die Beteiligten ein entsprechender Hinweis aufgenommen.

[38] Urteil v. 27. Oktober 2005 – 10 Sa 783/05

die Durchführung eines Eingliederungsmanagements im Sinne des § 84 Abs. 2 SGB IX nicht formelle Wirksamkeitsvoraussetzung für eine krankheitsbedingte Kündigung. Mit den Maßgaben in dieser Vorschrift wird im Fall der krankheitsbedingten Kündigung jedoch das dem Kündigungsrecht innewohnende Ultima-Ratio-Prinzip verstärkend konkretisiert. Dieses anerkannte Prinzip beinhaltet, dass die Kündigung nur als letztes Mittel auszusprechen ist, wobei zuvor eine Prüfung aller milderen Möglichkeiten durchzuführen ist. Die Personalvertretung kann daher im Zusammenhang mit einem fehlenden Eingliederungsmanagement grundsätzlich die Zustimmung zu einer krankheitsbedingten Kündigung verweigern, wenn eine solche nur mit Zustimmung des Personalrats ausgesprochen werden kann. Da Ziel des Eingliederungsmanagements vor allem ist, den Ausspruch einer Kündigung zu verhindern und Maßnahmen zur Überwindung der Arbeitsunfähigkeit zu erörtern und umzusetzen, kann dieses Ultima-Ratio-Prinzip bei Fehlen eines Eingliederungsmanagements nicht eingehalten werden. Die Kündigung wäre dann als unverhältnismäßig anzusehen und gemäß § 1 Kündigungsschutzgesetz sozialwidrig und unwirksam.

Da § 84 Abs. 2 SGB IX nicht auf Arbeitnehmer beschränkt ist, sondern dort ausdrücklich von Beschäftigten gesprochen wird, ist diese Vorschrift auch auf Beamte anzuwenden. Vor dem Hintergrund der o. g. Ausführungen ist daher grundsätzlich ein Eingliederungsmanagement vor einem Zurruhesetzungsverfahren einzuleiten bzw. durchzuführen. Ein Eingliederungsmanagement ist vor der amtsärztlichen Untersuchung zur Feststellung der Dienstfähigkeit einzuleiten. Ist ein solches nicht durchgeführt worden, wäre die Zurruhesetzung rechtswidrig. Auch hier könnte der Personalrat im Rahmen eines Mitbestimmungsverfahrens seine Zustimmung verweigern.

Verweigert dagegen ein Beschäftigter seine Zustimmung zur Durchführung des Eingliederungsmanagements, kann er sich im weiteren Verlauf nicht auf ein *fehlendes* Eingliederungsmanagement berufen.

Auswirkungen des Eingliederungsmanagements auf die *Personalakte*

Da der Arbeitgeber in einem eventuellen Kündigungsschutzverfahren die Durchführung des Eingliederungsmanagements darlegen muss, sind zumindest Eckdaten des Eingliederungsmanagements zur Personalakte zu nehmen. Diese Daten umfassen insbesondere Gesprächsangebote des Dienstherren mit Datum, Abschluss des Gesprächs mit Datum sowie den Abbruch der Gespräche mit Datum. Nur bei diesen Daten handelt es sich um Unterlagen, die mit dem Dienst-/Arbeitsverhältnis des Beschäftigten in einem unmittelbaren inneren Zusammenhang stehen und ihn betreffen. Regelungen zum Umgang mit diesen Daten

Die besonderen datenschutzrechtlichen Hinweise in dem Jahresbericht 2006 haben es ermöglicht, die Formulierungen und inhaltlichen Regelungen der DV Ges auf diese Erfordernisse abzustimmen. Für die Anwender und für die betroffenen Dienstkräfte besteht dadurch Klarheit und Sicherheit im Umgang mit den persönlichen Daten.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

finden sich in § 56 ff. Landesbeamtengesetz Berlin (LBG), der analog auf alle Beschäftigtengruppen im öffentlichen Dienst anzuwenden ist, sowie in § 28 Abs. 1 Nr. 1 und 2 BDSG i. V. m. § 2 Abs. 2 BlnDSG.

Alle übrigen Unterlagen über Gesprächsinhalte werden dagegen nicht Gegenstand der Personalakte, da sie den Betroffenen nicht unmittelbar in seinem Dienst-/ Arbeitsverhältnis betreffen (ähnlich wie bei Gerichtsentscheidungen, hier wird ebenfalls nur der Tenor Gegenstand der Personalakte). Die Aufbewahrungsfrist für diese Eckdaten richtet sich nach § 56 f. Abs. 2 LBG bzw. § 35 Abs. 2 Nr. 3 BDSG und sollte nicht länger als fünf Jahre betragen.

Die Aufbewahrungsfrist ist in der Dienstvereinbarung auf nur zwei Jahre begrenzt.

Die Gesprächsinhalte unterliegen dabei einer absoluten Geheimhaltungspflicht der Gesprächsteilnehmer bzw. des Integrationsteams. Gesprächsergebnisse sind nur dann den jeweils zuständigen Stellen mit Einverständnis des Betroffenen zu offenbaren, wenn es sich dabei um die konkrete Umsetzung von Hilfsangeboten (Arbeitsplatzveränderung, Hilfsmittel etc.) handelt.

Situation in der Berliner Verwaltung

Das Eingliederungsmanagement ist bereits seit Mai 2004 gesetzlich vorgeschrieben, steckt jedoch bezüglich seiner Anwendung und Umsetzung immer noch in den Kinderschuhen. So gibt es noch keine berlinweit verbindliche Regelung oder Rahmendienstvereinbarung zwischen dem Hauptpersonalrat und der Senatsverwaltung für Inneres, sondern nur einzelne Verfahrensanleitungen von verschiedenen Senatsverwaltungen. Insbesondere aus datenschutzrechtlicher Sicht erscheint es in höchstem Maße problematisch, wenn offensichtlich jede Senatsverwaltung bzw. jede öffentliche Stelle im Land Berlin ihre eigenen Vorstellungen zur Umsetzung des Gesetzes in Verfahrensanleitungen, Handlungshilfen etc. formuliert und damit hochsensibles Datenmaterial innerhalb Berlins unterschiedlich gehandhabt wird. Die Auswirkungen eines unsachgemäßen Umgangs mit Gesundheitsdaten haben dabei bestenfalls nur dienstrechtliche, in besonderen Fällen jedoch auch strafrechtliche Konsequenzen für die Beteiligten des Integrationsteams. Abgesehen davon bedeutet diese unterschiedliche Verfahrensweise bei ein und demselben Dienstherren auch eine erhebliche Rechtsunsicherheit für den Betroffenen, die die erfolgreiche Durchführung eines Eingliederungsmanagements infrage stellt.

Wir begrüßen und unterstützen daher ausdrücklich alle Bemühungen, durch Abschluss einer entsprechenden Rahmendienstvereinbarung zwischen dem Hauptpersonalrat und der Senatsverwaltung für Inneres, die hier eine besondere Verantwortung trägt, eine verbindliche Regelung zu schaffen, die die wichtigsten Umsetzungskriterien zum Eingliederungsmanagement landesweit festschreibt.

Die DV Ges wird gegenwärtig im Senat und anschliessend mit den Bezirken abgestimmt. Der breite Konsens ist schon wegen der Auswirkungen auf den Dienstbetrieb und wegen der einheitlich zu gestaltenden Organisation des Betrieblichen Gesundheitsmanagements eine Voraussetzung zur kurzfristigen Umsetzung. Der Senat folgt damit der Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit, dass auf diesem Gebiet, aber auch zum Komplex "Gesundheitsmanagement" insgesamt eine berlinweit einheitliche verbindliche Grundlage geschaffen werden muss.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

2.5 Server Based Computing

Server Based Computing – zurück zu den Wurzeln der zentralen Datenverarbeitung

Mit Server Based Computing (SBC) wird eine aktuelle Betriebsform moderner IT-Systeme bezeichnet, die im Prinzip die normalen lokalen Netze verändert und mit entfernten Ressourcen ergänzt.

Seit vielen Jahren beobachten wir im Jahresbericht die Entwicklung von Personal Computern auf der Grundlage der quantitativen Steigerung ihrer technischen Komponenten wie Prozessor, Arbeitsspeicher und Festplatte. Ein marktüblicher PC für das traute Heim, z. B. aus dem Angebot von Discountern, erreicht heute Werte, mit denen locker das Melderegister der Stadt Berlin betrieben werden könnte, gäbe es nicht neben quantitativen auch noch qualitative Aspekte und müsste das Melderegister nicht stadtweit online zur Verfügung stehen.

Auf jeden Fall stehen die quantitativen Leistungsmerkmale von Arbeitsplatzcomputern in keinem Verhältnis zu den Anforderungen, die Clients in Netzwerken erfüllen müssen. Wenn ein Client, wie in *Client-Server-Systemen* üblich, hauptsächlich mit einem zentralen Datenbestand arbeiten soll, benötigt er z. B. nur einen minimalen Bruchteil der heute meist verfügbaren Festplattenkapazität. Da liegt es nahe, über Konsequenzen dieses Missverhältnisses für Systemkonfigurationen nachzudenken.

Einige wichtige Hersteller haben deshalb Konzepte entwickelt, die zum Ziel haben, die Verarbeitungskapazitäten bei der Datenverarbeitung wieder mehr zentral vorzuhalten und an den Arbeitsplätzen die Kapazitäten zu verschlanken. Da die Intelligenz der Clients im Vergleich zu Arbeitsplatzcomputern ausgedünnt ist, spricht man von Thin Clients. Die dezentralen Systemkomponenten führen keine oder nur wenige eigenständige Prozesse aus, sie sind primär für die ergonomisch einwandfreie Präsentation der Verarbeitungsergebnisse da. Die Verarbeitungsergebnisse stehen also dort zur Verfügung, wo sie gebraucht werden, die Verarbeitung selbst erfolgt an anderer Stelle.

Zu diesen Konzepten gehören die Terminalserver-Lösung METAFRAME Server der Fa. CITRIX, das „Computing on Demand“ der Firma IBM, das „Stateless Computing“ mit „Thin Clients“ der Firma SUN und das „Server Based Comping“ der Firma Microsoft. Damit sind sicher nur die Marktführer genannt, andere Unternehmen bieten vergleichbare Lösungen an. Gemeinsam ist diesen Konzepten die Idee, zentrale IT-Dienstleistungen dezentral anzubieten, wo immer sie gebraucht werden. So wie der elektrische Strom kommt die IT-Dienstleistung aus der Steckdose, es

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

kommt überhaupt nicht mehr darauf an, woher sie tatsächlich kommt. Große Firmen wie Microsoft oder IBM betreiben weltweit nur noch wenige Rechenzentren (Data Center), die rund um den Globus die Firmenmitarbeiter mit den erforderlichen Anwendungen einheitlich versorgen.

Aus der Sicht des Datenschutzes bietet Server Based Computing zunächst Vorteile:

- Die Verlagerung von Verarbeitungsprozessen von den Clients auf den Server schließt alle Risiken aus, die durch Manipulationen an den Clients verursacht werden. Da dies bei Client-Server-Systemen ein wichtiges Sicherheitsproblem darstellt, ist durch die Umstellung von Verfahren auf Terminalserver-Konfigurationen ein wesentlicher Sicherheitsgewinn zu verzeichnen.

- Mit einer Terminalserver-Lösung können lokale Netzwerke sicher an das Internet angebunden werden. Wenn die lokalen Clients über einen gewidmeten Terminalserver mit dem Internet kommunizieren, können Angriffe aus dem Internet auf die lokalen Clients und damit bei den Anwendungen auf dem lokalen Netz nicht wirksam werden.

- Der Administrationsaufwand für die Clients wird erheblich reduziert, tendiert fast gegen Null. Damit fallen Fehlerquellen aus, die sich auf die Verfügbarkeit und Integrität der Datenverarbeitung auswirken können.

- Die Ausfallsicherheit von Clients wird dadurch verbessert, dass sie besser austauschbar sind und die Möglichkeit für Nutzer gegeben ist, auf andere Clients auszuweichen.

Es sind aber auch Nachteile in den Risikoanalysen und Sicherheitskonzepten zu beachten:

Die im Bericht dargestellten spezifischen Anforderungen an einen sicheren Einsatz von Server Based Computing werden bei der Erstellung der notwendigen IT-Sicherheitskonzepte beachtet.

- Bei einer konsequenten Terminalserver-Anwendung mit zentralem Server und spezialisierten Thin Clients hängt die Verfügbarkeit des Systems von der Verfügbarkeit des Servers ab. Ausweichlösungen, die auf dem Stand-Alone-Betrieb der Arbeitsplatzrechner beruhen – z. B. zum Weiterbetrieb der Office-Funktionen wie die Textverarbeitung –, gibt es dann nicht mehr.

- Server Based Computing verringert für die anwendenden Unternehmen die Transparenz der Datenverarbeitung. Wer die IT-Anwendungen „aus der Steckdose“ zieht, verliert die Kontrolle über die Sicherheit des Netzwerks, über das er versorgt wird. Ist der Server authentisch? Wie wirkt er auf die dezentralen Clients ein? Unternehmen, die ihre Datenverarbeitung über Server Based Computing ausge-

lagert haben, können die Fähigkeit verlieren, die unternehmenskritische Datenverarbeitung selbst unter Kontrolle zu halten. Dies steht im Widerspruch zu den Zielen der IT-Governance, insbesondere zu der Verpflichtung der Unternehmen, die Verantwortung für die Datenverarbeitung des Unternehmens selbst tragen und unternehmensbedrohende Risiken ausschließen zu können.

***Server Based Computing* – technische Ansätze**

Beim Server Based Computing bzw. beim Einsatz von Terminalserver-Konfigurationen werden zwar die Anwendungen auf einem zentralen Server verarbeitet, die Ausgabekanäle, wie beispielsweise die Bildschirmausgabe, werden jedoch auf einen entfernten Arbeitsplatz umgeleitet. Ein Server kann dabei eine Reihe von grafischen Logins parallel betreuen. Die Applikationen werden vom Administrator des Servers betreut. An dieser Stelle erfolgt auch die Zugriffskontrolle. Ein Arbeitsplatz kann Verbindungen zu einer Vielzahl von Servern aufbauen, sofern der Benutzer dazu berechtigt ist.

Die Clients, auch wenn sie selbst über entsprechende Rechenleistung verfügen, agieren lediglich als Ein- bzw. Ausgabegerät. Die Funktionalität entspricht prinzipiell der von einfachen „dummen“ Terminals, wie sie noch aus älteren Großrechner- oder UNIX-System-Konfigurationen bekannt sind. Hier ist auch der Zusammenhang mit dem Begriff „Terminalserver“ zu sehen. Im Gegensatz zum einfachen Terminal kann jedoch der „Terminal-Client“ seine Ressourcen wie seine Schnittstellen, den daran angeschlossenen lokalen Drucker, seine Soundkarte weiterhin nutzen. Mittlerweile wurden in vielen Produkten Zusatzfunktionen integriert, die auch die Nutzung der Peripherie des Clients durch den Server ermöglicht. Der Client ist sogar in der Lage, weiterhin die Aufgaben eines vollwertigen PC wahrzunehmen, sofern dieses gewollt wird und er entsprechend ausgestattet ist.

Der Ansatz, Funktionen von grundsätzlich dezentral organisierten Personal Computern zu zentralisieren, ist unter dem Stichwort "Netzwerk-Computer“ schon einmal verfolgt worden[39]. Diese Netzwerk-Computer sind Clients, deren lokale Ausstattungen stark reduziert wurden: Interne Massenspeicher werden nicht mehr gebraucht. Alles, was für die Verarbeitung benötigt wird, wird im Netz bereitgestellt. Der Netzwerkcomputer stellt die Benutzeroberfläche, dahingehend ist er optimiert.

Der damalige Ansatz scheiterte aus mehreren Gründen. Einerseits stieß die damals durchschnittlich verfügbare Netzwerkleistung von 10 Megabit/Sekunde schnell an ihre Kapazitätsgrenze. Das wurde im Be-

[39] JB 1997, 2.1

sonderen durch den Einzug von grafischen Benutzeroberflächen (z. B. Windows) deutlich. Diese benötigten sog. "virtuellen Arbeitsspeicher“, der standardmäßig auf Festplatten abgelegt wurde und einer sehr hohen Anzahl von Zugriffen ausgesetzt war. Nur wenige Maschinen reichten aus, um ein Netz zu überlasten. Andererseits war die damals zur Verfügung stehende Hardware nicht leistungsfähig genug, um dieses Problem etwa durch entsprechend hohe Arbeitsspeicherkapazitäten zu kompensieren.

Mittlerweile existieren verschiedene Produkte mit teilweise unterschiedlichen Ansätzen auf dem Markt. Allen Produkten ist gemein, das Clients mit unterschiedlichen Betriebssystemen eingesetzt werden können.

Microsoft Terminal Server benutzt zur Anbindung ein proprietäres Übertragungsprotokoll (RDP Daten - Port 3389). Das Produkt ist prinzipiell mit Einführung von Windows-2000-Server in das Betriebssystem integriert, muss aber extra lizenziert werden. Das RDP-Protokoll arbeitet komprimiert, aber unverschlüsselt. Ist eine Verschlüsselung notwendig oder gewünscht, muss auf Produkte anderer Anbieter ausgewichen werden. Ressourcen des Clients, wie beispielsweise ein Drucker, können innerhalb der SBC-Umgebung verwendet werden. Der Microsoft Terminalserver stellt dem Nutzer einen virtuellen Desktop zur Verfügung. Laut Ankündigung der Firma Microsoft soll der Terminalserver um zusätzliche Sicherheitsmerkmale ergänzt werden. Inzwischen wurde auch in die Betriebssystemreihe für Arbeitsplatzrechner eine stark eingeschränkte Version dieser Technologie für Administrationszwecke integriert.

Citrix MetaFrame nutzt zur Übertragung ein ebenfalls proprietäres Übertragungsprotokoll (ICA – nutzt diverse Ports). Durch Erweiterungen kann eine verschlüsselte Übertragung auf dem HTTPS (Port 443) erfolgen, sodass auf den Klienten nur ein Browser, der über diese Funktionalität verfügt, vorhanden sein muss. Die Möglichkeiten von Citrix Metaframe sind variabler und somit auch komplexer als die anderer Produkte.

VNC (Virtual Network Computing) ist eine weit verbreitete SBC-Software. Es können sowohl Rechner unter Unix als auch unter Windows durch den Server „ferngesteuert“ werden. Auch VNC verwendet ein eigenes nicht verschlüsseltes Protokoll, das aber im Gegensatz zu den kommerziellen Produkten offen ist. Um eine verschlüsselte Übertragung zu gewährleisten, kann das VNC-Protokoll durch das Open-SSH (Open-Secure Shell – Port 22) getunnelt (umgeleitet) werden. VNC wurde primär für das „Fernsteuern“ von Rechnern konzipiert, dieser Umstand führt bei der Servervariante von Windows zu einigen Einschränkungen, weil im Gegensatz zu den o. g. Produkten allen zugreifenden Klienten nur ein Desktop zur Verfügung

gestellt wird, den sich die Klienten teilen müssen. Die Unix/Linux-Variante ist von dieser Einschränkung nicht betroffen, da jeder Nutzer einen eigenen X-Server (grafische Bedienoberfläche) startet. Ein weiterer Nachteil von VNC ist die fehlende Unterstützung für die Übertragung von Audio- und Druckdaten.

Das Opensource-Project Free-NX wurde auf der Grundlage eines von der italienischen Firma No Machine entwickelten Protokolls entwickelt. Es bietet die Möglichkeit, auf die grafische Benutzeroberfläche von Unix-Rechnern (X-Server) auch über Verbindungen mit geringer Bandbreite zuzugreifen. Die Sicherheit von NX beruht auf der Verwendung des SSH-Protokolls bei der Übertragung von Daten und eines kryptografischen Verfahrens (Public Key Kryptografie) zum Zweck der Authentifizierung. Im Gegensatz zu VNC steht die gesamte Funktionalität des X-Systems zur Verfügung.

Das am meisten verbreitete Anwendungsszenario für SBC ist die Anbindung von Behörden- oder Unternehmensnetzen an ein Netz mit geringerem Sicherheitsniveau (z. B. Internet oder Berliner Landesnetz/MAN). Der prinzipielle Aufbau ist unabhängig von der eingesetzten Software immer gleich. Zwischen den beiden Netzen wird ein zusätzliches Grenznetz eingerichtet. Der Verkehr zwischen Grenz- und Behörden- bzw. Unternehmensnetz wird stark reglementiert, im Idealfall wird nur ein Protokoll benötigt, mit dem ausschließlich der Verbindungsaufbau zwischen den Clients des Behörden- bzw. Unternehmensnetzes zu den Servern gestattet wird. Den Servern werden lediglich die Rechte für Verbindungen in das „unsichere“ Netz erteilt. Eine direkte Verbindung der Clients zum „unsicheren“ Netz ist auszuschließen. Die Nutzer erhalten den Zugriff ausschließlich über dedizierte Clientprogramme, der im Idealfall mit einer sog. Sandbox-Umgebung vergleichbar ist. Eine Sandbox-Umgebung bezeichnet eine Laufzeitumgebung, in der Software vom Rest des Systems abgeschirmt, quasi in den Sandkasten gesetzt wird. Code, der in dieser Umgebung ausgeführt wird, kann keinen Schaden anrichten. Im Falle der Kompromittierung der Server ist das interne Netz somit nicht betroffen.

Die Unterschiede bei der Sicherheit ergeben sich zum einen daraus, ob das Protokoll verschlüsselte Kommunikation möglich macht oder nicht, und zum anderen aus den Möglichkeiten des eingesetzten Serverbetriebssystems. Citrix und Microsoft Terminalserver nutzen serverseitig Microsoft Windows als Betriebssystem, wogegen NX und VNC auf Linux beheimatet sind. Für VNC existiert zwar auch eine Windows-Server-Variante, deren Funktionalität aber soweit eingeschränkt ist, sodass sie hier nicht betrachtet wird (s.o.). Durch die Nutzung der Standardbetriebssysteme als Plattform ist SBC von deren Schwächen und Stärken abhängig.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Im Bereich der Linux-Betriebssysteme wurde in den letzten Jahren eine Technik entwickelt, die das nutzerbezogene Berechtigungssystem um ein dienste-/anwendungsbezogenes Berechtigungssystem erweitert. In der Fachwelt werden dafür Begriffe wie „SecurityEnhanced-Linux“, „AppArmor“, „RBAC“ oder „RSBAC“ verwandt. Grundlage dafür ist das Prinzip, dass anhand einer Regelbasis (Policy) entschieden wird, wer auf welche Systemteile welchen Zugang hat.

Die Policy wird vom Administrator vorgegeben und lässt sich von normalen Benutzern nicht beeinflussen. Dass Sicherheitseinstellungen sehr detailliert vorgenommen werden können, hat seinen Preis in einer beachtlichen Komplexität. Um ein Programm geschützt laufen zu lassen, muss ein Administrator jede Datei kennen, die der Prozess öffnet, und auch jedes Unterprogramm, das er aufruft. Die Komplexität steigt mit der Anzahl der installierten Dienste und Anwendungen, sodass in diesem Bereich ein großes Fachwissen unabdingbare Voraussetzung ist.

Der Einsatz dieser Technologie im SBC-Umfeld kann das Sicherheitsniveau beträchtlich verbessern.

Server Based Computing in den Berliner Behörden

Mit dem Aufkommen der Client-Server-Architekturen Mitte der 90er Jahre wurden auch in der Berliner Verwaltung die meisten informationstechnischen Anwendungen in diese dezentrale Betriebsform überführt. Dies führte auch zur Dezentralisierung der Entscheidungsstrukturen für den Einsatz der Informationstechnik in der Verwaltung und damit zu einer Diversifizierung der verwendeten Betriebs- und Anwendungssysteme. Inzwischen zeichnet sich ein Trend zurück zur Zentralisierung ab. Dies wird nicht bedeuten, dass die Datenverarbeitung ähnlich wie vor der Dezentralisierung vollständig zentral an einem Ort erfolgt. Vielmehr entwickelt sich eine hybride IT-Landschaft, in der versucht wird, die Vorteile von zentraler und dezentraler Datenverarbeitung zu nutzen. Dieser Trend basiert auf Server Based Computing.

Auch wir haben in diesem Jahr erfolgreich mit VNC ein solches System in unserer Dienststelle eingeführt. Damit konnte die bisherige Lösung, die den Einsatz von zwei völlig eigenständigen Netzen mit jeweils zwei getrennten Rechnern pro Arbeitsplatz voraussetzte, durch eine neue Lösung ersetzt werden, die eine wesentlich höhere Effizienz bei geringerem Administrationsaufwand bietet, ohne dass die Sicherheit eingeschränkt wird.

Ein weiteres Einsatzszenario ist die Verlagerung eines Verfahrens in eine SBC-Umgebung. In diesem Fall können ungewollte Wechselwirkungen des Fachverfahrens mit anderen auf den PC-Arbeitsplätzen instal-

Der Senat betrachtet die mit Server Based Computing (SBC) verbundenen technischen und betrieblichen Ansätze als wichtige Möglichkeit, den IT-Einsatz in der Berliner Verwaltung anforderungsgerecht zu gestalten. Die im Bericht dargestellten konkreten Einsatzformen sind Beispiele für eine erfolgreiche Umsetzung der SBC-Konzepte entsprechend den vorhandenen dezentralen Anforderungen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

lierten Anwendungen minimiert werden. Das Verfahren wird in einer „gekapselten“ Umgebung betrieben. Ein Beispiel für erfolgreiche Umsetzung dieses Konzepts ist das Sozialhilfe-Verfahren BASIS mit der Software PROSOZ. Durch die Umstellung auf eine Terminalserver-Umgebung wurden wesentliche Sicherheitslöcher des Verfahrens gestopft. Auch das Verfahren NOWI zur Verarbeitung von Ordnungswidrigkeiten im Nichtverkehrsbereich durch die Berliner Ordnungsämter, dessen Pilotanwendung im Bezirksamt Friedrichshain-Kreuzberg bevorsteht, nutzt eine solche Lösung.

Darüber hinaus hat die Senatsverwaltung für Inneres mit dem Projekt IT-Inn einen Terminalservice für die Funktionalitäten der Bürokommunikation eingerichtet, wobei das IT-Dienstleistungszentrum Berlin (ITDZ) als externer Dienstleister fungiert.

Der zentrale IT-Dienstleister des Landes Berlin (ITDZ) bietet seinen Kunden die Ausstattung und den Betrieb der IT-Infrastruktur vom Server bis zum Endgerät an (Dienstleistung ITIS – „IT-InSourcing“). Die Senatsverwaltung für Inneres und Sport nutzt diese Dienstleistung für den Betrieb ihrer IT-Infrastruktur. Hierbei bildet SBC die technische Basis.

Die Betriebsform ITIS hat mittlerweile in der Berliner Verwaltung - in unterschiedlicher Ausprägung - einen erheblichen Umfang erreicht und wird daher von der Senatsverwaltung für Inneres und Sport als bedeutsam angesehen

Insgesamt ist für die Berliner Verwaltung ein deutlicher Trend zur neuen Betriebsform des Server Based Computing festzustellen.

2.6 Datenschutz bei *Dokumentenmanagementsystemen*

Der Einsatz eines Dokumentenmanagementsystems (DMS) ist eine der wichtigsten Herausforderungen, der sich heute öffentliche Verwaltungen stellen müssen. Unterstützt durch die Entwicklungen beim eGovernment und zur Digitalisierung der Verwaltung, wie z. B. mit der Einführung der elektronischen Akte, bietet eine Vielzahl von Herstellern Dokumentenmanagementsysteme auf dem Markt an. Neben der Beschleunigung der Verwaltungsvorgänge ist ein wesentliches Ziel dieser Technologie, Informationen jeder Art, die in der Verwaltung vorhanden sind, erschließbar zu machen.

Bisherige IT-Verfahren, die datenschutzrechtlich beurteilt wurden, waren oftmals Fachverfahren, die nur Teilinformationen einer Akte oder eines Vorgangs und Verarbeitungsschritte enthielten. Die Ergebnisse waren für Nichtfachleute oft nur mit Zusatzinformationen verständlich. In Dokumentenmanagementsystemen werden jedoch nicht nur Daten, sondern auch aussagefähige Dokumente vorgehalten. Dadurch entsteht ein erhöhtes Risiko gegenüber konventionellen Verfahren, da kein Zusatzwissen erforderlich ist, um Informationen verstehen und verwerten zu können. In Dokumentenmanagementsystemen können Informationen auch fachübergreifend bereitgehalten werden. Dieses bringt jedoch Gefahren für das Recht auf in-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

formationelle Selbstbestimmung mit sich. Mit Dokumentenmanagementsystemen können automatisiert aus einer Datensammlung durch vielfältige Datenverknüpfungen und -kombinationen sowie durch die Erstellung von Hypothesen und deren Überprüfung bisher völlig unbekannte Informationen gewonnen werden. Insbesondere die gezielte Zusammenführung personenbezogener Daten aus unterschiedlichen Datenquellen und ihre Auswertung ermöglichen die Bildung von Persönlichkeitsprofilen.

Besondere Datenschutzrisiken ergeben sich, wenn die Papierakte durch eine elektronische Akte ersetzt wird, deren Dokumente in einem Dokumentenmanagementsystem vorgehalten werden. In diesem Fall führen die Such- und Auswertungsfunktionen eines Dokumentenmanagementsystems, insbesondere wenn eine Volltextrecherche zugelassen ist, zu bisher nicht oder nicht in dem Umfang gegebenen Aussagen zu einer Person. Statt viele Seiten einer Papierakte durchlesen zu müssen und vielleicht noch andere Akten hinzuzuziehen, könnten dann ohne Aufwand Daten von Bürgerinnen und Bürgern aus verschiedenen Lebens- bzw. Verwaltungsbereichen zusammengeführt werden, ohne dass Zusatzwissen erforderlich wäre. Bisher ist eine umfassende Recherche zu einer bestimmten Person nur mit erheblichem Aufwand möglich. Mit Einführung der elektronischen Akte in einem Dokumentenmanagementsystem ist dies jedoch theoretisch auf Knopfdruck möglich. Auch wird es für Bürgerinnen und Bürger noch schwieriger zu durchschauen, wer Zugang zu ihren Daten hat.

Dokumentenmanagementsysteme können aber auch zur Verhaltens- und Leistungskontrolle der Mitarbeiterinnen und Mitarbeiter genutzt werden. Durch die Einführung der elektronischen Akte werden sämtliche Bearbeitungsschritte elektronisch abgebildet. Es entsteht eine Vielzahl von Protokoll- und Verfahrensdaten, die mitarbeiterbezogen ausgewertet werden können.

Der Arbeitskreis eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat von einer Arbeitsgruppe die Orientierungshilfe "Datenschutz bei Dokumentenmanagementsystemen" erarbeiten lassen[40]. Die Orientierungshilfe stellt die datenschutzrechtlichen und -technischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur des Dokumentenmanagementsystems als Basiskomponente des eGovernment vor. Sie soll dazu beitragen, dass bei dem Einsatz eines Dokumentenmanagementsystems die Anforderungen von Datenschutz und Datensicherheit im Blick bleiben, und praktische Hinweise dafür geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können.

Der Einsatz von Dokumentenmanagement- und Vorgangsbearbeitungssystemen (DMS/VBS) ist integraler Bestandteil der IT-Landesstrategie. Die Senatsverwaltung für Inneres und Sport bereitet derzeit ein DMS-Konzept vor. Darin wird untersucht, welche organisatorischen, technischen, rechtlichen und wirtschaftlichen Rahmenbedingungen für einen flächendeckenden Einsatz eines Dokumentenmanagement- und Vorgangsbearbeitungssystems in der Berliner Verwaltung zu schaffen sind.

Der sichere Einsatz eines DMS bildet einen wichtigen Aspekt dieses Konzeptes. Der Senat betrachtet daher die Orientierungshilfe – und die im Bericht enthaltenen Ausführungen - als eine wichtige Grundlage, um die

[40] http://www.datenschutz.hessen.de/o-hilfen/DsimDokumanagement.pdf

Im Folgenden werden einige der wesentlichen datenschutzrechtlichen und -technischen Aspekte bei der Einführung und dem Einsatz von Dokumentenmanagementsystemen dargestellt.

Was ist ein Dokumentenmanagementsystem?

Ein Dokumentenmanagementsystem verwaltet elektronisch und nichtelektronisch erzeugte Dokumente über deren gesamten Lebenszyklus hinweg. Es organisiert dabei Entwurf und Erstellung, Weitergabe und Verteilung, Auffinden, Ablage und Übergabe an ein Archiv oder Löschung der Dokumente sowie Auswertung und Zuordnung von Informationen aus den Dokumenten. In einem Dokumentenmanagementsystem existieren zu jedem Dokument zusätzliche Informationen, sog. Metadaten. Diese enthalten beschreibende Informationen von Dokumenten, Vorgängen oder Akten. Dies kann z. B. das Aktenzeichen, der Erstellzeitpunkt, der Bearbeiter oder der Ablageort sein.

Mit der Einführung eines Dokumentenmanagementsystems sollen verschiedene Ziele verwirklicht werden. Durch den Umstieg von der reinen Papierakte bzw. der teilelektronischen Akte zur vollständigen elektronischen Akte entsteht ein einfacher und aktueller recherchierbarer Bearbeitungsstand mit vielfältigen Auswertungsmöglichkeiten. Die Schnelligkeit der Bearbeitung wird gesteigert, da Transportzeiten entfallen, Dokumente mittels Workflow direkt zu den entsprechenden Bearbeitern geführt und parallel von mehreren Bearbeitern genutzt werden können.

Organisatorische Rahmenbedingungen

Die Nutzung eines Dokumentenmanagementsystems verändert die Arbeit in jeder Behörde erheblich. Dies nicht nur, weil es sich um ein zentrales Arbeitsmittel handelt, sondern auch, weil es die Abläufe innerhalb der verantwortlichen Stelle und an den Schnittstellen nach außen erheblich verändert. Erster Schritt vor der Einführung eines Dokumentenmanagementsystems muss deshalb eine gründliche organisatorische Vorbereitung sein. Gleiches gilt für Unternehmen, die ein Dokumentenmanagementsystem einführen.

Hauptaugenmerk aller Untersuchungen sind die zu speichernden Dokumente. Der umfassenden Analyse des tatsächlichen Schutzbedarfs der zu verarbeitenden Dokumente kommt eine Schlüsselrolle zu.

Das Berliner Datenschutzgesetz und das Bundesdatenschutzgesetz unterscheiden nur zwischen Kategorien bzw. Arten personenbezogener Daten, für die besondere Schutzvorschriften bestehen, und den übrigen

notwendigen Anforderungen an einen sicheren Einsatz von DMS bereits in der jetzigen Konzeptphase und bei den weiteren notwendigen Schritten ausreichend berücksichtigen zu können.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Daten, bei denen keine weitere Gewichtung vorgenommen wird. Dementsprechend muss für alle personenbezogenen Daten - unabhängig von ihrer besonderen Schutzwürdigkeit - in jedem Fall zunächst ein Grundschutz gewährleistet sein. Besondere Kategorien personenbezogener Daten sind nach § 6 a BlnDSG bzw. § 3 Abs. 9 BDSG personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen oder die die Gesundheit oder das Sexualleben betreffen. Diese Daten dürfen nur verarbeitet werden, wenn angemessene Garantien zum Schutz des Rechts auf informationelle Selbstbestimmung bestehen und eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, dies erlaubt.

Daten, die dem Sozialgeheimnis, dem Personalaktengeheimnis oder einem anderen besonderen Amts- oder Berufsgeheimnis unterliegen, sind nach spezialgesetzlichen Regelungen besonders geschützt, was sich in einem erhöhten Schutzbedarf niederschlägt. Die Verarbeitung oder Nutzung von Personalaktendaten in einem Dokumentenmanagementsystem ist nur zulässig, wenn die maßgeblichen Regelungen zur Personalaktenführung in den Beamtengesetzen des Bundes und der Länder dem nicht entgegenstehen.

Sollte die Feststellung des Schutzbedarfs der Dokumente ergeben, dass die vom Grundschutzkatalog empfohlenen Maßnahmen allein nicht ausreichend sind, so müssen zusätzliche Maßnahmen ergriffen werden. Dieses kann z. B. eine Verschlüsselung der Dokumente im Dokumentenmanagementsystem bedeuten. Liegen Schriftformerfordernisse vor, muss zudem eine qualifizierte Signatur angebracht werden.

Die sich aus diesen Fragen ergebenden Erkenntnisse der Voruntersuchungen müssen in ein Organisationskonzept überführt werden, das neben Festlegungen zur Aufbau- und Ablauforganisation auch Aussagen zum Funktionsumfang des künftigen Dokumentenmanagementsystems enthalten muss. Hier sind die unerlässlichen Funktionen bzw. Fähigkeiten des künftigen Systems ebenso festzulegen wie die notwendigen Beschränkungen, z. B. der Auswertungs- und Recherchemöglichkeiten.

Der datenschutzgerechte Einsatz eines Dokumentenmanagementsystems erfordert klare Festlegungen, wer für welche Aufgaben verantwortlich ist und wer die Verantwortung für die Vollständigkeit und Korrektheit von Daten und Verfahren trägt. Hierfür muss ein verfahrensbezogenes Datenschutz- und Datensicherheitskonzept erarbeitet werden. Das Datenschutz- und Datensicherheitskonzept basiert auf der Analyse des Schutzbedarfs der Dokumente.

Eine mangelhafte Benutzer- und Rechteverwaltung

kann dazu führen, dass Unberechtigten Zugang zu personenbezogenen Daten gewährt wird. Dieses kann z. B. durch die Nutzung einer gemeinsamen Benutzerkennung von mehreren Beschäftigten passieren oder wenn Personen innerhalb eines spezifischen Verfahrens über Rechte verfügen, die sie zur Aufgabenerledigung nicht benötigen. Daher muss ein detailliertes Rollen- und Rechtekonzept Bestandteil des Datenschutz- und Datensicherheitskonzeptes sein und manipulationssicher im Dokumentenmanagementsystem implementiert werden.

Durch die Möglichkeiten der Inhaltskontrolle und Protokollierung in Dokumentenmanagementsystem können die Benutzer prinzipiell überwacht und ihre Leistung und ihr Verhalten kontrolliert werden. Deshalb ist die frühzeitige Beteiligung der Personalvertretung und des behördlichen Datenschutzbeauftragten vor der Einführung eines solchen Systems unerlässlich.

Datenschutzrechtliche Anforderungen an ein Dokumentenmanagementsystem

Für die Verwendung eines Dokumentenmanagementsystems sind die allgemeinen datenschutzrechtlichen Grundsätze zu beachten: Personenbezogene Daten dürfen nur erhoben, verarbeitet oder sonst genutzt werden, wenn und soweit das zur rechtmäßigen Erfüllung der Aufgaben der Daten verarbeitenden Stelle für den gesetzlich zugelassenen oder durch Einwilligung eröffneten Zweck erforderlich ist. Die Daten verarbeitende Stelle hat diejenigen technischen und organisatorischen Maßnahmen zu ergreifen, die erforderlich sind, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten. Die datenschutzrechtliche Kernfrage beim Einsatz eines Dokumentenmanagementsystems ist, wie wirksam verhindert wird, dass

- Dokumente unzulässig im Dokumentenmanagementsystem gespeichert werden oder bleiben,

- auf im Dokumentenmanagementsystem gespeicherte Dokumente unzulässig zugegriffen werden kann,

- Dokumente manipuliert werden und

- auf Protokolldaten der Beschäftigten zur Leistungs- und Verhaltenskontrolle unzulässig zugegriffen wird.

Technisch-organisatorische Anforderungen

Die Umsetzung der organisatorischen und rechtlichen Rahmenbedingungen muss durch technische Maßnahmen ergänzt werden, damit das Recht auf informationelle Selbstbestimmung der Betroffenen beim Einsatz eines Dokumentenmanagementsystems gewährleistet werden kann. Auf der Basis einer Risi-

koanalyse muss ein Sicherheitskonzept erstellt werden. Es muss folgende Sicherheitsziele beinhalten:

Vertraulichkeit

Es ist in jeder Phase der Datenverarbeitung sicherzustellen, dass nur befugte Personen Daten zur Kenntnis nehmen können. Es sind daher restriktive Zugriffsberechtigungen zu vergeben. Sind an die Dokumente hohe Vertraulichkeitsanforderungen zu stellen, ist eine Verschlüsselung vorzusehen. Zum einen ist eine Verschlüsselung der Daten zu fordern, die über ein Kommunikationsnetz übertragen werden, und zwar unabhängig davon, ob es sich um ein lokales oder ein öffentliches Netz handelt. Zum anderen sind auch die bei den Daten haltenden Systemen gespeicherten Daten zu verschlüsseln. Nur so kann verhindert werden, dass z. B. Systemadministratoren oder Wartungspersonal Kenntnis von den Daten erhalten.

Authentizität und Integrität

Mit dem elektronischen Signieren eines Dokumentes zur Sicherstellung der Authentizität wird gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokumenteninhalts bescheinigt. Wird ein Dokument elektronisch unterschrieben, wird damit nicht nur die Urheberin oder Urheber bestätigt, sondern auch, dass das Dokument echt sowie inhaltlich korrekt und vollständig ist. Weiterhin sichert das der elektronischen Signatur zugrunde liegende Verfahren die Erkennung einer nachträglichen Veränderung eines Dokumentes.

Weitere Mittel zur Sicherstellung der Integrität sind beispielsweise die Versionsverwaltung von Dokumenten und die Protokollierung von Änderungen.

Verfügbarkeit

Die Sicherstellung der Verfügbarkeit hängt u. a. von der Art der Datenhaltung ab. Bei einer zentralen Datenhaltung sind gängige Maßnahmen, wie z. B. regelmäßige Datensicherung, Einsatz von Spiegelservern u. Ä. vorzusehen. Bei einer dezentralen Datenhaltung hängt die Verfügbarkeit des Gesamtsystems von der Verfügbarkeit der einzelnen Teilsysteme ab. Es sind also in allen beteiligten Systemen die oben dargestellten Maßnahmen zu realisieren.

Revisionsfähigkeit

Eine Möglichkeit für die Gewährleistung der Revisionsfähigkeit ist das elektronische Signieren von Dokumenten, da hiermit die Verantwortlichkeit bzw. Urheberschaft anerkannt wird. Da der Inhalt eines signierten Dokumentes nachträglich nicht mehr verändert werden kann, ohne dass die Signatur nicht mehr zum Dokument passt, können inhaltliche Änderungen nur in Form von Ergänzungen einem Dokument angefügt werden. Wird das Ursprungsdokument zusammen mit

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

den Ergänzungen wiederum digital signiert, kann die Historie eines Dokumentes manipulationssicher festgehalten werden.

Durch geeignete technische und organisatorische Maßnahmen kann für jeden Ablaufschritt in einem Dokumentenmanagementsystem eine datenschutzgerechte Ausgestaltung erfolgen. Dies betrifft die Vorbereitung der in Papierform eingehenden Post**,** das Scannen, die Behandlung der in elektronischer Form eingehenden Post, die Metadateneingabe, das Workflow-Management ebenso wie die Recherche. Gerade die Recherche birgt besondere datenschutzrechtliche Risiken.

Der wesentliche datenschutzrechtliche Aspekt der Recherche betrifft die vollständige Beachtung der vorhandenen *Zugriffsrechte*. Die Zweckbindung der Datenverarbeitung erfordert neben der exklusiven Zuweisung von Zugriffsrechten z. B. auch eine Einschränkung der Suchfunktion. Die Gefahr liegt unter anderem in der Möglichkeit der Verknüpfung der verschiedenen Such- und Auswertungsmöglichkeiten, wobei dies auch automatisiert erfolgen kann. Ein Zugriff auf Meta- oder Inhaltsdaten, für die keine Zugriffsberechtigung existiert, ist deshalb technisch auszuschließen.

Erforderlich ist eine präzise Beschreibung der Suchfunktion und der Maßnahmen, die sicherstellen, dass über die Suchfunktion nicht die datenschutzrechtlichen Grundsätze der Zweckbindung und der Erforderlichkeit sowie der gebotene Vertraulichkeitsschutz umgangen werden können. Das Suchergebnis darf sich nur auf diejenigen Dokumente und Metadaten beziehen, zu denen auch eine Zugriffsberechtigung besteht. Ein Suchergebnis darf nicht als Treffer angezeigt werden, wenn keine Zugriffsberechtigung besteht. Eine leere Trefferliste muss demnach nicht bedeuten, dass es kein Ergebnis zur Suchanfrage gab, sondern vielmehr, dass es keine Treffer in der Zugriffsberechtigung der abfragenden Person gibt. Es kann auch erforderlich sein, den Zugriff nur auf die Metadaten zu erlauben, auf die dazugehörigen Dokumentinhalte jedoch nicht. Es kann ggf. auch erforderlich sein, den Zugriff nur auf eine begrenzte Zahl von Feldern der Metadaten zuzulassen.

Dokumentenmanagementsysteme bergen Risiken für das Recht auf informationelle Selbstbestimmung, die nur durch entsprechende technische und organisatorische Rahmenbedingungen beherrscht werden können.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

3 Öffentliche Sicherheit

3.1 Polizei

3.1.1 Umsetzung von Entscheidungen des Bundesverfassungsgerichtes im Polizeirecht

Bereits im März 2004 hat das Bundesverfassungsgericht mit seiner Entscheidung zum „*Großen Lauschangriff*“[41] festgestellt, dass das gesprochene Wort, das im Rahmen des *Kernbereichs privater Lebensgestaltung* in einer Wohnung geäußert wird, absoluten Schutz genießt. Diese Feststellung hat das Bundesverfassungsgericht in einer Entscheidung bestätigt, in der es die Regelungen des Niedersächsischen Sicherheits- und Ordnungsgesetzes zur vorbeugenden Telefonüberwachung weitgehend für nichtig erklärt hat[42].

Die Entscheidungen hatten Auswirkungen auf das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG). Es mussten Regelungen getroffen werden, die sichern, dass Kommunikationsinhalte des höchstpersönlichen Lebensbereiches nicht von staatlichen Stellen belauscht, gespeichert und verwertet werden dürfen[43]. Sie sind unverzüglich zu löschen, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist. Auch die Erhebung im Rahmen eines durch ein Amts- oder Berufsgeheimnis geschützten Vertrauensverhältnisses war zu regeln.

Das Abgeordnetenhaus von Berlin hat noch vor Ende der letzten Legislaturperiode erfreulicherweise das ASOG entsprechend novelliert[44]. Dabei wurden unsere Anregungen weitgehend aufgegriffen und wesentliche grundrechtssichernde Maßnahmen getroffen. Nur die ebenfalls gebotene Erstreckung des Kernbereichsschutzes auf den Einsatz verdeckter Ermittler der Polizei und auf den Verfassungsschutz steht noch aus[45].

Der Senat wird die Anregung des Berliner Beauftragten für Datenschutz und Informatiosfreiheit prüfen.

Zusätzlich wurde unsere Kritik an den Aufzeichnungen von Notrufen in der Leitstelle der Berliner Feuerwehr[46] berücksichtigt und eine Rechtsgrundlage dafür geschaffen.

Es ist zu begrüßen, dass der Berliner Gesetzgeber die Vorgaben des Bundesverfassungsgerichts für den Schutz des Kernbereichs der persönlichen Lebens-

[41] Urteil v. 3. März 2004 - 1 BvR 2378/98

[42] Urteil v. 27. Juli 2005 – 1 BvR 668/04

[43] Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 19

[44] 7. Gesetz zur Änderung des ASOG, GVBl. 2006, 930

[45] JB 2005, 1.2

[46] JB 2004, 4.1.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

gestaltung bei polizeilichen Lauschangriffen umgesetzt hat. Dieser Schutz muss auch bei anderen verdeckten Ermittlungsmaßnahmen von Polizei und Verfassungsschutz gewährleistet werden.

3.1.2 Datenabrufverordnung Berlin-Brandenburg

Der Senat beabsichtigt, eine Verordnung über den automatisierten Datenzugriff zwischen den Polizeien der Länder Berlin und Brandenburg zu erlassen. Damit soll die länderübergreifende Kriminalitätsbekämpfung verbessert werden.

Mit der Datenabrufverordnung Berlin-Brandenburg soll Dienstkräften der Gemeinsamen Ermittlungsgruppe der Polizeien der Länder Berlin und Brandenburg (GEG) oder Verbindungsbeamten des Landes Berlin unter bestimmten Voraussetzungen der Zugriff im Rahmen eines automatisierten Abrufverfahrens auf das Berliner *Polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS)* eröffnet werden.

Im Rahmen unserer Beteiligung wiesen wir darauf hin, dass die geplante Verordnung in ihrer ursprünglich vorgesehenen Form datenschutzrechtlich aus verschiedenen Gründen problematisch sei. Zwei wesentliche Kritikpunkte lauteten:

Bei der Festlegung der zu übermittelnden Daten wurde keine Aufzählung der einzelnen, zu übermittelnden Datenfelder vorgenommen. Es wurden Oberbegriffe genannt, die beispielhaft erläutern und mit Zusätzen wie beispielsweise „usw." versehen sind. Die Senatsverwaltung für Inneres begründete diese beispielhafte Aufzählung zwar mit dem Erhalt einer notwendigen Flexibilität: Es solle nicht bei jedem geänderten Unterfall des Anwendungsbereiches einer Datenart die Verordnung geändert werden müssen. Eine nicht abschließende Aufzählung der Datenfelder ist jedoch zu unbestimmt, um den gesetzlichen Anforderungen zu genügen. Zweck einer Verordnung ist es gerade, in Konkretisierung abstrakter gesetzlicher Vorgaben bestimmte Festlegungen zu treffen. Nach der ursprünglich geplanten Regelung hätte es der Verwaltung jedoch offengestanden, nach ihrem Belieben neue Datenfelder hinzuzufügen, was der eigentlichen Funktion der Verordnungsbefugnis, Rechtssicherheit zu schaffen, vollends zuwidergelaufen wäre.

Darüber hinaus sollte mit einer Öffnungsklausel auch anderen als den o. g. Dienstkräften der GEG oder Verbindungsbeamten der Zugang zu den Berliner Daten in POLIKS eröffnet werden. Damit wäre der Kreis der Abrufberechtigten indirekt vergrößert worden, was die zuvor getroffene Festlegung eines begrenzten Kreises unterlaufen hätte. Vor dem Hintergrund einer immer möglichen konventionellen Anfrage bei der Berliner Polizeidienststelle hielten wir die Erweiterung des Kreises der Abrufberechtigten auch für nicht erforder-

Der Erlass einer Rechtsverordnung für den Zugriff Brandenburger Polizeibeamter auf Berliner Datenbestände, jetzt POLIKS, wird bereits seit vielen Jahren betrieben. Grund dafür ist, dass Berlin und Brandenburg als gemeinsamer kriminalgeografischer Raum anzusehen sind und sich Straftäter nicht an den Landesgrenzen ausrichten. Dies führte auch zur Bildung gemeinsamer Ermittlungsgruppen mit dem Ziel der Bekämpfung bestimmter Kriminalitätsphänomene.

Die entsprechende Rechtsverordnung befindet sich weiterhin im Entwurfsstadium. Zutreffend ist, dass die Gespräche hierzu noch nicht abgeschlossen sind.

Aufgrund der Kritik des Berliner Beauftragten für Datenschutz und Informationsfreiheit an der nach seiner Auffassung zu unbestimmten Festlegung der abzurufenden Datenfelder wurden diese durch Aufzählung der zu Personen, Sachen und Institutionen gespeicherten und abrufbaren Daten weitest möglich präzisiert.

Der Kreis der Abrufberechtigten ist auf die Polizeidienstkräfte des Landes Brandenburg beschränkt, die der Gemeinsamen Ermittlungsgruppe der Polizeien der Länder Berlin und Brandenburg angehören oder als Verbindungsbeamte bei der Berliner Polizei beschäftigt sind.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

lich. Diesen Kritikpunkt hat die Senatsverwaltung zum Anlass genommen, den Entwurf der Rechtsverordnung zu überarbeiten. Die Gespräche sind noch nicht abgeschlossen.

Bei einem automatisierten Abrufverfahren muss die Art der abzurufenden Daten hinreichend bestimmt und abschließend festgelegt werden. Wird eine Regelung über einen abrufberechtigten Personenkreis erlassen, darf diese nicht durch unbestimmte Öffnungsklauseln aufgeweicht werden.

3.1.3 *Videoaufnahmen* der Polizei bei Hausdurchsuchungen und Versammlungen?

Ein Bürger beschwerte sich darüber, dass die ermittelnden Polizeibeamten anlässlich einer Hausdurchsuchung Videoaufzeichnungen von den Wohnräumen angefertigt hatten.

Das Anfertigen der Videoaufnahmen war unzulässig. Das hat die Polizei eingeräumt und die Videobänder gelöscht. Losgelöst von dem konkreten Einzelfall haben wir auf folgende Rechtslage in Bezug auf Videoaufzeichnungen durch polizeiliche Beweissicherungs- und Festnahmeeinheiten (BFEs) hingewiesen:

Im repressiven Bereich ist schon das Fotografieren in der Wohnung bei Hausdurchsuchungen nur in Ausnahmefällen zulässig,[47] nämlich als milderes Mittel zu einer Beschlagnahme (§ 94 StPO) und als unabwendbares Beweissicherungsmittel (§§ 160 Abs. 2, 163 StPO). Lediglich zum Zweck der Dokumentation der ordnungsgemäßen Durchführung dürfen keine – statischen – Fotografien gefertigt werden. Beim Anfertigen eines Videos wird durch die Möglichkeit der umfassenden Erfassung von privater Lebensführung und -gestaltung tiefer in die Privatsphäre eingegriffen als bei einer Fotografie. Das Anfertigen von Videoaufnahmen stellt somit die einschneidendere Maßnahme dar. Sie ist folglich auch nur dann zulässig, wenn der verfolgte Zweck nicht schon durch ein ausnahmsweise zugelassenes Fotodokument erreicht werden kann.

Das Gleiche gilt erst recht, wenn die Polizei zur Gefahrenabwehr eine Wohnung betritt. Eine Videoaufzeichnung ist nach § 42 ASOG nur dann zulässig, wenn sie verhältnismäßig ist. Das heißt, sie muss zur Gefahrenabwehr geeignet und erforderlich sein, und es darf kein milderes Mittel (beispielsweise das Anfertigen einer Fotografie) ausreichen.

Beim Anfertigen von Videoaufnahmen bei Versammlungen und Veranstaltungen hat die Polizei die Anforderungen der §§ 19 a, 12 a Versammlungsgesetz zu beachten. Videoaufzeichnungen sind nur dann zulässig, wenn tatsächliche Anhaltspunkte die Annahme

Es besteht Konsens darüber, dass das Anfertigen von Videoaufnahmen bei Wohnungsdurchsuchungen einen erheblichen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt und nur nach einer sorgfältigen Einzelfallprüfung in Ausnahmefällen durchgeführt werden darf. Die Berliner Polizei orientiert sich bei Wohnungsdurchsuchungen an diesen strengen Maßstäben und handelt dabei insbesondere nach dem Grundsatz der Verhältnismäßigkeit.

Beim Anfertigen von Videoaufnahmen bei Versammlungen und Veranstaltungen vertreten Teile der Literatur die Auffassung, dass Übersichtsaufnahmen nur unter den Voraussetzungen des § 12 a VersG zulässig sind. Der Senat folgt jedoch der vom Versammlungs-

[47] OLG Celle – 3 VAs 20/84; LG Hamburg – 622 Qs 11/04

rechtfertigen, dass von den Teilnehmern erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Eine Speicherung der Aufnahmen zu Ausbildungszwecken der Polizei ist unzulässig, da das Versammlungsgesetz abschließend regelt, dass eine Speicherung nur zur Strafverfolgung in Betracht kommt (§ 12 a Abs. 1 Nrn. 1 und 2).

Schon das Fotografieren ist während einer Wohnungsdurchsuchung grundsätzlich nicht erlaubt. Lediglich im Fall besonders rechtfertigender Umstände kann das ausnahmsweise zulässig sein. Der Einsatz von Videotechnik kann deshalb allenfalls dann zulässig sein, wenn das Anfertigen von Fotos zulässig ist, aber der verfolgte Zweck damit nicht erreicht werden kann.

3.1.4 Ausschreibungen im *Schengener Informationssystem (SIS)*

Die Gemeinsame Kontrollinstanz für das Schengener Informationssystem hat beschlossen, in allen Vertragsstaaten eine Kontrolle des Verfahrens der Ausschreibungen nach Artikel 99 Schengener Durchführungsübereinkommen (SDÜ) durchzuführen. Das SDÜ sieht die Ausschreibung von Personen und Kraftfahrzeugen zur verdeckten Registrierung oder gezielten Kontrolle vor (Artikel 99). Eine solche Ausschreibung ist zur Gefahrenabwehr und zur Strafverfolgung zulässig, wenn konkrete Anhaltspunkte für die Planung oder die Begehung von Straftaten außergewöhnlichen Umfanges vorliegen. Grund für die Kontrolle war das erhebliche Abweichen der Anzahl der Ausschreibungen in den einzelnen Ländern. In der Bundesrepublik wurde die Kontrolle vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und von den Datenschutzbeauftragten der Länder durchgeführt.

Zum Zeitpunkt der Auswertung des Datenbestandes im März entfielen 46 Ausschreibungen auf Berlin. Zum Prüfungszeitpunkt im Juni waren noch neun Datensätze vom Landeskriminalamt Berlin in das SIS eingestellt. 38 Datensätze aus zwei Verfahren waren bereits im April wegen Fristablaufes gelöscht worden. Bei unserer Prüfung konnte kein Verstoß gegen die Anforderungen des Artikel 99 SDÜ festgestellt werden.

Die Prüfung der Datenschutzbeauftragten der anderen Bundesländer, in denen die Polizei zum Teil erheblich mehr Datensätze in das SIS eingestellt hatte, führte überwiegend ebenfalls zu keinen Beanstandungen. Vereinzelt wurde festgestellt, dass bestehende Unterschiede zwischen Artikel 99 SDÜ und dem nationalen Recht nicht berücksichtigt wurden. Teilweise ist es in anderen Bundesländern Praxis, eine nach nationalem Recht zulässige polizeiliche Beobachtung regelmäßig in das SIS zu übernehmen. Das betrifft auch die nach nationalem Recht zulässige – im SDÜ aber nicht vorgesehene – Beobachtung von Kontaktpersonen. Weiter erfolgte in Einzelfällen die Ausschreibung sche-

gesetzgeber ausweislich der Begründung zum Versammlungsgesetz (BT-Drs. 11/4359, Seite 17) sowie von anderen Teilen der Literatur vertretenen Meinung, dass Übersichtsaufnahmen zur Leitung und Lenkung des Polizeieinsatzes und zu Zwecken der Aus- und Fortbildung keiner versammlungsrechtlichen Ermächtigungsgrundlage bedürfen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

matisch ohne Darlegung einer konkreten Gefahr. Verlängerungsanträge für die Fortdauer der Speicherung wurden in einigen Fällen nicht hinreichend begründet oder gar nicht dokumentiert. Betraf die Ausschreibung Gruppen, wurden keine personenscharfen Begründungen gegeben, sondern nur solche, die die ganze Gruppe betrafen. In Einzelfällen wurden die Löschtermine falsch gesetzt. Teilweise unterblieb die nach Landesrecht vorgesehene Unterrichtung der Betroffenen nach Abschluss der Maßnahme.

Die Ausschreibung im Schengener Informationssystem richtet sich ausschließlich nach dem zugrunde liegenden Durchführungsübereinkommen und nicht nach nationalem Recht.

Der Senat teilt die Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit, dass Ausschreibungen nach Art. 99 SDÜ sich ausschließlich nach dieser Befugnisnorm richten. Nationales Recht kann nur dann und insoweit zur Anwendung kommen, als Art. 99 SDÜ dies zulässt.

3.1.5 Das Lichtbild und die Auskunft

Ein Bürger beschwerte sich darüber, dass einem Zeugen ein Foto von ihm in einer Wahllichtbildvorlage gezeigt worden war. Gegen ihn wurde zwar vor längerer Zeit strafrechtlich ermittelt; diese Wahllichtbildvorlage stand aber in keinem Zusammenhang mit seiner Person. Das Foto sei lediglich zur Auffüllung verwandt worden. Im Übrigen trug sein Rechtsanwalt vor, dass der Staatsschutz eigene Lichtbildsammlungen unterhalten würde. Außerdem sei ein Auskunftsersuchen, das sich ausdrücklich auch auf INPOL-Anwendungen bezogen habe, mit einem allgemeinen Hinweis darauf, dass in den kriminalpolizeilichen Sammlungen der Berliner Polizei keine weiteren Daten bzw. Unterlagen zur Person seines Mandanten vorhanden seien, beschieden worden.

Nach längerem Schriftwechsel mit dem Polizeipräsidenten in Berlin hat erst die Senatsverwaltung für Inneres klarstellen müssen, dass die Einbeziehung von Fotos des nicht tatverdächtigen Bürgers im Widerspruch zu ihrer vorgegebenen Vorgehensweise – Lichtbilder von in konkreten Verfahren Unverdächtigen dürfen nicht in einer Wahllichtbildvorlage verwandt werden - steht. Wie es dennoch dazu kommen konnte, ließ sich aufgrund des Zeitablaufs nicht mehr feststellen. Die Senatsverwaltung für Inneres hat den Polizeipräsidenten in Berlin erneut auf die Vorgabe hingewiesen und um ausnahmslose Beachtung gebeten.

Im Übrigen traf die Aussage des Rechtsanwalts zu, dass der Polizeiliche Staatsschutz eine Teillichtbildvorlagenkartei für politisch motivierte Tatverdächtige ausländischer Herkunft als Teil der erkennungsdienstlichen Sammlung der Berliner Polizei führte. Die Kartei bestand aus mehrbändigen, nach Geschlechtern getrennten Mappen und wurde Anfang 2004 in die

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Lichtbilddatei BIDAVIS[48] übernommen. Das Karteimaterial ist vernichtet worden.

Außerdem hatte eine andere Landespolizei in dem vom Bundeskriminalamt geführten Verfahren INPOL Daten über den Betroffenen gespeichert.

Die Senatsverwaltung für Inneres teilt unsere Auffassung, dass mit einer Standardformulierung auf das Bundeskriminalamt verwiesen werden sollte, die offen lässt, ob Daten gespeichert sind oder nicht. Damit würde die Entscheidungskompetenz über die Auskunftserteilung, die bei INPOL-Anwendungen – soweit es sich nicht um die Berliner Landesdaten handelt - bei dem Bundeskriminalamt oder der einstellenden Polizeibehörde liegt, nicht unterlaufen. Die Senatsverwaltung für Inneres hat den Polizeipräsidenten in Berlin angewiesen, in künftigen Fällen so zu verfahren.

Der Polizeipräsident in Berlin hat den geforderten Hinweis auf die Zuständigkeit des Bundeskriminalamtes für Auskünfte aus INPOL-Dateien als Standardformulierung in seine Mitteilungen anlässlich von Auskunftsersuchen aufgenommen.

Die Lichtbilder von in konkreten Verfahren Unverdächtigen dürfen nicht in eine Wahllichtbildvorlage aufgenommen werden. Mit einer Standardformulierung, die offen lässt, ob tatsächlich Daten gespeichert sind oder nicht, sind Betroffene bei Auskunftsersuchen über INPOL-Anwendungen auf die Zuständigkeit des Bundeskriminalamtes hinzuweisen.

3.1.6 Aufgaben, Arbeitsweisen und Datenverarbeitungsbefugnisse der Vermisstenstelle

Die Bearbeitung von Vorgängen über *Vermisste* und Unbekannte ist in der Regel Gefahrenabwehr und richtet sich deshalb nach den Vorschriften des ASOG. Lediglich bei unbekannten Toten obliegt es der Staatsanwaltschaft, diese zu identifizieren. Hier richtet sich die Datenverarbeitung ausnahmsweise nach der Strafprozessordnung
Wir haben im Zusammenhang mit der Tätigkeit der Vermisstenstelle beim Polizeipräsidenten auf unsere folgende Rechtsauffassung hingewiesen:

- Die Überwachung der Telekommunikation in Form der Ortung des Vermissten per Handy lässt sich nicht auf eine polizeirechtliche Ermächtigungsgrundlage stützen; das ASOG enthält für eine solche Maßnahme keine Befugnis. Auch das Telekommunikationsgesetz (TKG) selbst bietet keine Ermächtigungsgrundlage für eine entsprechende Gefahrenabwehrmaßnahme.

- Eine Erhebung personenbezogener Daten von Vermissten bei Ärzten oder Zahnärzten halten wir auf der Grundlage des ASOG nur bei Vorhandensein hinreichender Anhaltspunkte für das Vorliegen einer Gefahr für zulässig. Das ist beispielsweise

In Umsetzung der Koalitionsvereinbarung 2006 – 2011 erarbeitet der Senat derzeit einen Gesetzentwurf, um die Befugnis der Polizei, suizidgefährdete oder vermisste Personen über die Ermittlung der Standortdaten eines Mobilfunktelefons orten zu können, auf eine gesetzliche Grundlage zu stellen.

Es besteht Konsens, dass die Erhebung personenbezogener Daten bei Ärzten, die Auskunft über Kontenbewegungen bei Banken sowie das Betreten und Durchsuchen von Wohnungen durch die Polizei in Vermisstenfällen nur bei Vorliegen einer Gefahr zulässig sind. Eine Erweiterung dieser Befugnisse ist bei der anstehenden Änderung des ASOG nicht beabsichtigt.

Im Rahmen der anstehenden Änderung des ASOG plant der Senat auch die Schaffung einer Befugnisnorm für die Erhebung von DNA-Vergleichsproben in Ver-

[48] Bilddatenverarbeitungs- und Informationssystem

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

dann der Fall, wenn

- zu befürchten ist, dass der Vermisste Straftaten begehen wird,
- eine Verletzung des Aufenthaltsbestimmungsrechtes der Sorgeberechtigten vorliegt oder
- zu befürchten ist, dass der Vermisste selbst einer Gefahr für Leib oder Leben ausgesetzt ist, weil eine Selbsttötungs- oder Selbstverstümmelungsabsicht vorliegt oder er Opfer einer Straftat zu werden droht.

In welchen Fällen die Datenerhebung bei Ärzten in Vermissten-Fällen auch erforderlich ist, kann abstrakt nicht beurteilt werden, sondern ist an den Umständen des Einzelfalls auszurichten. Dabei hat die Polizei eine Abwägung zwischen den gefährdeten Gütern und dem Interesse an einer effektiven Gefahrenabwehr vorzunehmen. Der Arzt selbst hat zu entscheiden, ob und ggf. in welchem Umfang er die Auskunft erteilt. Eine unbefugte Offenbarung durch ihn ist strafbewehrt (§ 203 StGB).

- In Bezug auf die Auskunft über Kontenbewegungen bei Banken gelten die gleichen Feststellungen wie zu den Ärzten. Die Bank hat zu prüfen, ob sie nach den für sie geltenden Vorschriften eine Übermittlungsbefugnis hat. In Betracht kommen könnte hier § 28 Abs. 3 Nr. 2 BDSG (zweckfremde Übermittlung oder Nutzung der Daten zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit).

- Die *Aufenthaltsbestimmung* von Kindern und Jugendlichen enthält einen verfassungsrechtlichen Konflikt (Grundrechte der Eltern - Grundrechte der Minderjährigen). Diese Grundrechtskollision stellt jedoch nur dann tatsächlich ein Problem dar, wenn der erkennbare Wille des Vermissten deutlich wird, von der Bestimmung seines Aufenthaltsortes abzusehen, und zudem nicht auf eine Gefahr für Leib oder Leben des Vermissten geschlossen werden kann. Das wird insbesondere dann der Fall sein, wenn die Vermissten ersichtlich freiwillig den elterlichen Lebenskreis verlassen haben. In diesen Fällen neigen wir dazu, dennoch das elterliche Fürsorge- und Aufenthaltsbestimmungsrecht als vorrangig anzusehen. Die Kollision stellt sich jedoch in allen anderen Fällen nicht, in denen aufgrund von Tatsachen eine konkrete Gefahr für Leib oder Leben des Vermissten oder - sofern die Gefahr vom Vermissten ausgeht - für eine andere Person besteht. In diesem Zusammenhang ist die gesonderte Unterrichtungspflicht gegenüber den Eltern zu beachten (§ 42 Abs. 5 ASOG).

- Für das Betreten der Wohnung von *Pädophilen* kommt § 36 Abs. 1 ASOG[49] als Rechtsgrundlage in

misstenfällen.

Die Aufbewahrung abgeschlossener Vermisstenvorgänge in der Kriminalpolizeilichen Personenakte (KPA) ist nicht zu beanstanden. Die KPA ist eine personenbezogene Sammlung von Dokumenten in POLIKS. Sie wird über namentlich bekannte Personen angelegt, die als Tatverdächtige oder Vermisste in Erscheinung getreten sind oder die einen Suizid versucht haben, und somit Anlass für kriminalpolizeiliche Ermittlungen gegeben haben. Innerhalb der KPA sind die Vermisstenvorgänge von denen, die der präventiven oder repressiven Bekämpfung von Straftaten dienen, durch Einrichtung eines eigenen Ordners getrennt.

[49] Betreten und Durchsuchen von Wohnungen

Betracht. Nach den qualifizierten tatbestandlichen Anforderungen (gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person) müssen entsprechende Tatsachen vorliegen. Dies wird in der Regel der Fall sein, wenn Tatsachen die Annahme rechtfertigen, dass Vermisste sich gegen ihren Willen in den Räumen der Störer befinden. Bei Gefahr im Verzug bedarf es der richterlichen Anordnung ausnahmsweise nicht.

- Die Akten über Vermisste werden so lange aufbewahrt, bis der Vermisste wieder aufgefunden wird. Nach der Erledigung wird der Vorgang komplett an die Aktenhaltung abgegeben und Bestandteil der Kriminalakte. Nach Ablauf der Prüffrist ist zu prüfen, ob eine weitere Speicherung der Daten zur Aufgabenerfüllung erforderlich ist (§ 48 ASOG i. V. m. der Prüffristenverordnung - PrüffristenVO). Das bedeutet, dass auch bei den unaufgeklärten Fällen spätestens nach Ablauf der Frist diese Prüfung vorzunehmen ist. Sofern eine weitere Aufbewahrung erforderlich ist, sind die Gründe dafür zu dokumentieren. Eine erneute Prüfung hat dann in fünf Jahren zu erfolgen. Die Aufbewahrung des Vermissten-Vorganges nach dessen Erledigung in der Kriminalakte halten wir aus den bekannten Gründen[50] für unzulässig.

- Veröffentlichungen von Fotografien Vermisster in den Medien sind Einzelangaben über persönliche und sachliche Verhältnisse einer natürlichen Person und somit personenbezogene Daten (§ 4 Abs. 1 BlnDSG). Sie lassen eine Identifizierung und Aussagen über das Erscheinungsbild einer Person zu. Wegen der Schwere des Eingriffes ist die Öffentlichkeitsfahndung nur bei Vorliegen einer Gefahr für Leib oder Leben zulässig.

Der Polizeipräsident in Berlin teilt unsere Auffassung mit einer Ausnahme: Zur Aktenhaltung besteht weiterhin ein Dissens. Der Polizeipräsident in Berlin hat die Senatsverwaltung für Inneres gebeten, dem Abgeordnetenhaus den Entwurf eines ASOG-Änderungsgesetzes mit dem Ziel der Schaffung der notwendigen Datenverarbeitungsbefugnisse für die Vermisstenstelle vorzulegen. Dazu ist es wegen des Ablaufes der Legislaturperiode nicht mehr gekommen.

Für die Arbeit der Vermisstenstelle sind die erforderlichen Datenverarbeitungsbefugnisse zu schaffen.

3.1.7 Informationsaustausch zwischen Polizei und Schule

Da in der Vergangenheit wiederholt Schulen an Polizeidienststellen herangetreten sind, um Informationen über straffällig gewordene Schüler und ihre Opfer zu

[50] JB 1999, 4.1.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

erhalten, hat der Polizeipräsident in Berlin ein Merkblatt entworfen und uns vorgelegt. Unsere Anregungen und Wünsche sind in der Endfassung des Merkblatts berücksichtigt worden.

Mit Einleitung des Strafverfahrens obliegt es grundsätzlich der Justiz, ob sie die Schule über einen jugendlichen Tatverdächtigen informiert. Nach dem Jugendgerichtsgesetz (JGG) und den sog. Mitteilungen in Strafsachen (MiStra) wird die Schule nur in "geeigneten Fällen" von der Einleitung und dem Ausgang eines Strafverfahrens in Kenntnis gesetzt (§ 70 JGG i. V. m. Nr. 33 MiStra). Gemäß einer Verfügung des Leitenden Oberstaatsanwalts von Berlin ist eine Mitteilung in solchen Fällen zu prüfen, in denen die Schule die Möglichkeit erhalten muss, der Gefahr eines negativen Einflusses auf Mitschüler begegnen zu können. In Betracht kommt sie bei Vergehen nach dem Betäubungsmittelgesetz, Sexual- oder Körperverletzungsdelikten, Verstößen gegen das Waffengesetz oder wenn Straftaten durch die Führungsansprüche von Jugendgangs durchgesetzt werden sollen. Sofern bereits eine Mitteilung über die Einleitung des Verfahrens geboten erscheint, sind die Sicherheit des Tatverdachtes und die Konsequenzen der Mitteilung für den Schüler und die Schule zu berücksichtigen. Ob eine Mitteilung geboten und damit zulässig ist, muss stets anhand einer Einzelfallbetrachtung geprüft werden.

Unabhängig hiervon hat die Polizei eigene Mitteilungsbefugnisse. Dies gilt für die Abwehr einer Gefahr, beispielsweise soweit ein jugendlicher Täter Drohungen gegen Mitschüler oder Lehrpersonal geäußert hat. Eine Mitteilung kommt aber auch in Betracht, wenn wegen der Schwere der Tat ein hoher Präventionsbedarf besteht, der eine Information der Schulleitung unerlässlich erscheinen lässt. Das ist regelmäßig beim Drogenhandel oder bei gefährlicher Körperverletzung durch den Schüler der Fall. Dort erscheint ein Zuwarten auf die zeitlich deutlich spätere Unterrichtung durch die Justiz unter präventiven Aspekten problematisch, weil die Schulen die Möglichkeit erhalten sollen, ihre anderen Schüler zu schützen. Auch dies ist stets einzelfallabhängig zu prüfen. Eine weitgehend "automatische" Meldung selbst bei Bagatellstraftaten, wie von einigen Schulen gewünscht, kommt nicht infrage. Das gilt erst recht hinsichtlich weiterer polizeilicher Vorerkenntnisse, insbesondere weiterer Straftaten ohne schulischen Bezug.

Die geltenden Regeln für die Mitteilungen von Staatsanwaltschaft und Polizei über straffällige oder gefährliche Schüler an ihre Schulen sind ausreichend. Sie müssen nur angewandt werden.

Wie in dem Bericht dargestellt, sollen nach den derzeit geltenden Vorschriften die Schulen in geeigneten Fällen von der Einleitung und dem Ausgang eines Strafverfahrens in Kenntnis gesetzt werden. Dieses Verfahren wurde in diversen interministeriellen Gremien gefordert und in den zuständigen Verwaltungen diskutiert. In der Praxis wurden bisher nur in wenigen Ausnahmefällen Informationen von Staatsanwaltschaft und Polizei an Schulen weitergeleitet, die es Schulen ermöglichen können, Sicherheitsrisiken, die von einzelnen Schülern ausgehen (z. B. Drogenhandel, gefährliche Körperverletzung, Sexualstraftaten außerhalb von Schulen), präventiv im Vorfeld zu kennen, um entsprechend aufmerksam sein zu können. Aus welchem Grund einzelne Schulen - wie dargestellt - eine Meldung aller Straftaten ihrer Schülerinnen und Schüler wünschen, ist dem Jahresbericht nicht zu entnehmen. Entsprechende Anfragen oder Anregungen aus den Schulen sind der zuständigen Senatsverwaltung nicht bekannt.

3.2 Verfassungsschutz

Im Bereich des Verfassungsschutzes standen im Be-

Die Vorbehalte des Berliner Beauftragten für Daten-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

richtszeitraum die Beratungen auf Bundesebene über das Gesetz zur Ergänzung des *Terrorismusbekämpfungsgesetzes*[51] und das *Antiterrordatei*-Gesetz[52] im Mittelpunkt unseres Interesses. Beide Gesetze sind inzwischen in Kraft getreten, bleiben allerdings erheblichen verfassungsrechtlichen und datenschutzrechtlichen Bedenken ausgesetzt.

Der zugrunde liegende Gesetzentwurf zur Ergänzung des Terrorismusbekämpfungsgesetzes „zieht" gemäß seiner Zielsetzung „die Konsequenzen aus einer durchgeführten Evaluation, die das Bundesministerium des Innern durchgeführt hat"[53].

Wir halten bereits die äußeren Rahmenbedingungen dieser Evaluierung für kritikwürdig. Der Evaluierungsbericht befindet sich auf einem Stand, der eine Auswertungslücke von mehr als eineinhalb Jahren aufweist. Weiterhin ist die Evaluation nicht durch eine unabhängige Institution, sondern durch die Bundesregierung und die ihr nachgeordneten Behörden durchgeführt worden. Eine solche „Evaluation in eigener Sache" führt naturgemäß zu Ergebnissen, welche die Rechtspositionen der evaluierten Stellen im Wesentlichen stützen. Abgesehen von diesen äußeren Rahmenbedingungen ist die Evaluation überdies einseitig auf die Effizienz der Maßnahmen ausgerichtet und damit lückenhaft. Beispielsweise werden zur Qualität der Beeinträchtigung von Grundrechten regelmäßig lediglich die Anzahl der betroffenen *Beschuldigten* aufgeführt und dann anschließend Ausführungen zu den Eingriffsschwellen gemacht. Es liegt auf der Hand, dass eine solche Interessenabwägung durch die Nichtberücksichtigung unverdächtiger Betroffener notwendig einseitig zugunsten der Interessen der handelnden Sicherheitsbehörden verschoben wird. Diese nur beispielhaft aufgeführten Mängel der Evaluation dokumentieren die Notwendigkeit von Evaluationen durch unabhängige Institutionen.

Inhaltlich zu kritisieren ist weiterhin die vorgesehene Umgestaltung und Erweiterung der Befugnisse von Verfassungsschutzbehörden und des Bundesnachrichtendienstes zu Auskunftsverlangen. Sie reichen nunmehr über den Zweck der Terrorismusabwehr hinaus zu einer Regelbefugnis bei der Erfüllung nahezu aller ihnen übertragenen Aufgaben. Dies verstößt gegen die Anforderungen des Verhältnismäßigkeitsgrundsatzes.

Darüber hinaus soll der Bundesnachrichtendienst die Befugnis erhalten, wie das Bundesamt für Verfassungsschutz Auskünfte bei inländischen Stellen einzuschutz und Informationsfreiheit beziehen sich auf die Gesetzgebung des Bundes. Der Senat sieht die Notwendigkeit einer effektiven Bekämpfung des auch Berlin unmittelbar betreffenden internationalen Terrorismus mit allen rechtstaatlichen und von der Verfassung gedeckten Mitteln als zwingende gegeben an, um die Sicherheit der Bevölkerung zu gewährleisten. Ungeachtet dessen sieht es der Senat als selbstverständlich an, darauf zu achten – und damit dem Anliegen des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu entsprechen -, dass bei der Schaffung entsprechender Gesetze die strikte Beachtung der Verhältnismäßigkeit gewahrt bleibt.

---

[51] BGBl. I 2007, 2

[52] Artikel 1 des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder – Gemeinsame Dateien-Gesetz –, BGBl. I 2006, 3409

[53] vgl. Bericht der Bundesregierung zu den Auswirkungen der nach Art. 22 Abs. 2 des Terrorismusbekämpfungsgesetzes befristeten Änderung des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Art. 10-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des § 7 Abs. 2 BKA-Gesetzes

holen. Der Gesetzentwurf zielt damit auf eine parallele Ausgestaltung der Auskunftsbefugnisse des Bundesnachrichtendienstes mit denen des Bundesamtes für Verfassungsschutz ab. Die erheblichen Persönlichkeitsbeeinträchtigungen aufgrund dieser neu geschaffenen Doppelzuständigkeit sind absehbar.

In Bezug auf die Erweiterungen der Befugnisse des Bundesnachrichtendienstes ist es weiterhin unverständlich, dass der Gesetzgeber nicht besondere Mechanismen des Schutzes von missbräuchlichem Handeln vorgesehen hat, wie es gerade nach den jüngsten Vorfällen der rechtswidrigen Ausforschung von Journalisten durch den Bundesnachrichtendienst nahe gelegen hätte. Vielmehr verzichtet der Gesetzentwurf bewusst auf die Fortführung der bisherigen rechtsstaatlich begründeten Regelungen über die Anordnung und Kontrolle der Befugnisse. Da der Bundesnachrichtendienst weit unterhalb der Schwelle des Verdachts tätig werden kann, lässt die Aufweichung von rechtsstaatlich begründeten Regeln über die Anordnung und Kontrolle von Befugnissen eine erhebliche Ausweitung der Überwachungsmaßnahmen durch den Bundesnachrichtendienst befürchten. Diese Regelung genügt deshalb nicht den Anforderungen an eine grundrechtssichernde Verfahrensgestaltung, wie sie das Bundesverfassungsgericht in ständiger Rechtsprechung festgestellt hat.

Besonders problematisch ist die vorgesehene Befugnis des Bundesamts für Verfassungsschutz, Personen zur europaweiten verdeckten Registrierung im Schengener Informationssystem ausschreiben zu lassen. Damit kann der Verfassungsschutz der Sache nach Personen weit unterhalb des Terrorverdachts in ganz Europa zur polizeilichen Beobachtung ausschreiben. Bezugspunkt ist dabei nicht nur die Terrorismusabwehr, sondern das gesamte Aufgabenspektrum des Verfassungsschutzes. Mit dieser Befugnis erhält der Verfassungsschutz nicht nur Zugriff auf polizeiliche Informationssysteme, sondern mittelbar auch polizeiliche Befugnisse. Eine solche Befugniserweiterung verstößt gegen das Prinzip der Trennung von Polizei und Nachrichtendienst. Nach diesem Prinzip verfolgen Polizei und Nachrichtendienste unterschiedliche Aufgaben: Die Polizei hat Gefahren abzuwehren, Störungen zu beseitigen und Straftaten zu verfolgen. Demgegenüber obliegen den Verfassungsschutzämtern und Nachrichtendiensten traditionell eher „strategische Aufklärungsaufgaben“, die der Sicherung des Bestandes der Bundesrepublik Deutschland dienen. Eine Entscheidung des Gesetzgebers zur Ausweitung von Datenübermittlungen zwischen Polizei und Nachrichtendiensten muss deshalb stets unter strenger Beachtung des Zweckbindungsprinzips und der aufgabenbedingt unterschiedlichen Befugnisvoraussetzungen erfolgen.[54]

[54] BVerfGE 100, 313 (383 ff.)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Aus diesen Gründen begegnet auch das Gesetz zur Errichtung Gemeinsamer Dateien von Polizeibehörden und *Nachrichtendiensten* des Bundes und der Länder gravierenden verfassungsrechtlichen Bedenken, auf die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 26./27. Oktober 2006 hingewiesen hat[55]. Danach sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Gegenüber der bisherigen Rechtslage sieht die Anti-Terror-Datei ganz erhebliche Erweiterungen des Datenaustausches vor. Besonders bedenklich ist die Verpflichtung der handelnden Behörden, bestimmte umfangreiche Daten in die gemeinsame Datei einzustellen. Bislang ist hierbei nicht ersichtlich, dass der Gesetzgeber hinreichend berücksichtigt hat, dass Nachrichtendienste in der Anti-Terror-Datei auch Personen erfassen würden, bei denen nur auf „weichen", nicht bewiesenen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Bereits ein relativ loser Kontakt zu einem Nachbarn kann zur Einstellung von Daten in die Anti-Terror-Datei führen. Mit anderen Worten: Ein Betroffener kann schnell in die Anti-Terror-Datei geraten, er wird es dann aber sehr schwer haben, aus ihr gelöscht zu werden. Insbesondere der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste ist deshalb auch im Hinblick auf das verfassungsrechtlich begründete Trennungsgebot problematisch. Es dürfen sogar Angaben zur Religionszugehörigkeit in der Anti-Terror-Datei gespeichert werden, soweit diese im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind. Ob ein solcher Fall vorstellbar ist, muss bezweifelt werden. Wahrscheinlicher ist hingegen, dass durch die Speicherung dieses sensitiven Datums Angehörige einer bestimmten Religion stigmatisiert werden.

Es zeichnet sich ab, dass das Bundesministerium des Innern einzelne verabscheuungswürdige Verbrechen zum Anlass nehmen wird, die Sicherheitsgesetze noch weiter gehend zu verschärfen, ohne dass dies einen nennenswerten Sicherheitsgewinn zur Folge hätte. Neben der geplanten *Vorratsspeicherung* von Telekommunikations- und Internetverbindungsdaten[56] soll beispielsweise bereits ein Referentenentwurf auf die Abänderung des Autobahnmautgesetzes abzielen, die das strikte Verbot der Verwendung von *Autobahnmautdaten* zu Strafverfolgungszwecken lockern soll. Beide Gesetzesvorhaben würden bei ihrer Realisierung eine flächendeckende Überwachung aller Internetnutzer bzw. Autobahnnutzer zur Folge haben. Im

[55] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006", S. 16

[56] vgl. dazu 10.1.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Sinne einer freiheitlich-demokratischen Gesellschaft wäre der Gesetzgeber gut beraten, solche Gesetzentwürfe sorgfältig daraufhin zu überprüfen, ob sie in Anbetracht der massiven Eingriffe in die Freiheitsrechte auch unverdächtiger Bürger tatsächlich unentbehrlich sind.

Der Senat ist aufgerufen, sich im Bundesrat dafür einzusetzen, dass der Bundesgesetzgeber bei der Schaffung von Sicherheitsrecht das rechte Augenmaß nicht verliert.

4 Ordnungsverwaltung

4.1 Meldewesen

4.1.1 Das neue *Meldegesetz*. – später Teilerfolg für den Datenschutz

Vor Jahren haben wir die Frage gestellt, ob das Ende einer unendlichen Geschichte in Sicht ist[57]. Erst im Spätsommer 2006 ist die von uns seit Jahren geforderte Anpassung an bundesrechtliche Vorgaben vollzogen worden. Im Wesentlichen wurden dabei die Regelungen des Melderechtsrahmengesetzes (MRRG) unverändert in Landesrecht umgesetzt.

Der Gesetzgeber hat mit dem neuen Berliner Meldegesetz die Rechte der Einwohner erheblich gestärkt. Auf unseren Vorschlag hin hat das Abgeordnetenhaus von Berlin zwei Regelungen beschlossen, die in der Bundesrepublik Deutschland einmalig sind: Zum einen hat der Bürger jetzt erstmals die Möglichkeit, eine Person seines Vertrauens zu benennen, die im Unglücks- oder Todesfall zu benachrichtigen ist. Deren Daten werden in seinem Datensatz im Melderegister gespeichert. Zum anderen kann der Bürger künftig bei An- oder Ummeldungen darüber entscheiden, ob seine Daten an Adressbuchverlage weitergegeben werden sollen und in welcher Form (in gedruckten oder elektronischen Verzeichnissen) sie veröffentlicht werden dürfen. Er kann auf diese Weise unerwünschte *Direktwerbung* begrenzen. Bereits vor der Verabschiedung des neuen Berliner Meldegesetzes hatte das Bundesverwaltungsgericht in einer Entscheidung zum Hamburgischen Meldegesetz[58] festgestellt, dass Meldepflichtige der Weitergabe ihrer Daten für Marketingzwecke generell ohne Angaben von Gründen widersprechen können. Diese Rechtsprechung müssen jetzt auch die Berliner Meldebehörden beachten.

Einem anderen Vorschlag, der das zentrale Auskunftsrecht betrifft, ist das Abgeordnetenhaus von Berlin nicht gefolgt: Es bleibt dabei, dass der Bürger nicht

Die im Jahr 2006 verabschiedete Novelle zum Meldegesetz wurde in den zuständigen Ausschüssen des Abgeordnetenhauses eingehend erörtert, sodass der Senat für eine erneute Kommentierung einzelner Aspekte der Gesetzesnovelle keine Veranlassung sieht.

[57] JB 2004, 4.2.1

[58] Urteil v. 21. Juni 2006 – 6 C 5.05

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

erfährt, welchen privaten Stellen die Meldebehörde eine einfache Melderegisterauskunft erteilt hat. Dazu gehören Familiennamen, Vornamen, Doktorgrade, gegenwärtige Anschriften und die Tatsache, dass der Einwohner verstorben ist. Die Verwaltung hat die Auffassung vertreten, dass eine Protokollierung dieser Auskünfte mit Blick auf den damit verbundenen Arbeits- und Technikaufwand unverhältnismäßig sei. Angesichts der zentralen, auch verfassungsrechtlich begründeten Bedeutung des datenschutzrechtlichen Informationsrechts des Betroffenen ist diese Argumentation nicht nachvollziehbar.

Das Meldewesen ist im Rahmen der *Föderalismusreform.* in die ausschließliche Gesetzgebungskompetenz des Bundes überführt worden[59]. Dazu wurde eine Ar-beitsgruppe eingerichtet. Deren Aufgabe besteht darin, Vorschläge für die Schaffung der rechtlichen Voraussetzungen für eine bundeseinheitliche, IT-basierte Neugestaltung der Melderegisterstruktur zu erarbeiten.

Wir werden uns dafür einsetzen, dass die neuen Regelungen im Berliner Meldegesetz, die Feststellungen des Bundesverwaltungsgerichtes und die Pflicht zur Protokollierung einfacher Melderegisterauskünfte in ein künftiges Bundesmeldegesetz übernommen werden.

4.1.2 Das automatisierte Abrufverfahren für die BVG

Die BVG strebte eine Zugriffsmöglichkeit auf das Melderegister an, um mit ihr die Identität von Fahrgästen feststellen zu können, die ohne gültigen Fahrausweis und ohne Personaldokument angetroffen werden. Vor allem wegen der fehlenden Eignung von Meldedaten zur *Identitätsfeststellung* wurde die BVG nicht in den Kreis der abrufberechtigten Stellen in die DVO-MeldeG aufgenommen. Da eine Einwilligung des Betroffenen eine gleichberechtigte Alternative zur materiell-rechtlichen Regelung ist, wurde ein in der Bundesrepublik Deutschland wohl einmaliges automatisiertes Abrufverfahren auf freiwilliger Basis[60] eingerichtet. Das Ergebnis einer Stichprobenuntersuchung zeigte allerdings, dass sehr oft keine den Datenabruf legitimierende schriftliche Einwilligung vorgelegt werden konnte. Die BVG hat die hohe Zahl an fehlenden Einwilligungserklärungen darauf zurückgeführt, dass die Prüfung zu einem Zeitpunkt stattgefunden habe, zu dem das Verfahren gerade eingeführt wurde. Inzwischen habe sich alles eingespielt und die Fehlerquote sei rückläufig.

Diese Darlegung widerspricht den Ergebnissen einer erneuten stichprobenartigen Nachprüfung, die wir im

Der Senat bedauert, dass es weiterhin zu datenschutzrechtlichen Problemen bei der Durchführung des auto-

[59] Art. 73 Abs. 1 Grundgesetz i. d. F. des Gesetzes zur Änderung des Grundgesetzes v. 28. August 2006, BGBl. I, 2034

[60] JB 2005, 4.2.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Oktober 2006 durchgeführt haben. Dabei konnten noch weniger Einwilligungsformulare vorgelegt werden als bei der ersten Stichprobe. Daneben sind uns Einwilligungen vorgelegt worden, die nicht wirksam erteilt worden sind: teilweise fehlte die Unterschrift oder sie erfolgte durch eine andere Person als den Betroffenen. Überdies sind häufig zusätzliche, nicht erforderliche Daten erhoben und gespeichert worden (beispielsweise Krankenversicherungsnummer).

Die BVG ist dringend gehalten, Maßnahmen zu ergreifen, die eine datenschutzkonforme Gestaltung des automatisierten Abrufverfahrens gewährleisten. Angesichts der wiederholt festgestellten datenschutzrechtlichen Mängel sind die gebotenen Maßnahmen zur Qualitätssicherung zeitnah umzusetzen.

matischen Abrufverfahrens durch die BVG gekommen ist. Die BVG steht im Dialog mit dem Beauftragten für Datenschutz und Informationsfreiheit. Sie hat weitere organisatorische Maßnahmen eingeleitet, um den Anforderungen des Berliner Datenschutzgesetzes, trotz der schwierigen Ausgangssituation vor Ort, gerecht werden zu können. Verstöße, die Mitarbeiter der BVG oder Fremddienstleister zu vertreten haben, werden konsequent verfolgt. Ergänzend prüft die BVG, ob die Einbindung der Einverständniserklärung in elektronischer Form bereits bei der Datenerhebung erfolgen kann.

Die beanstandeten Zusatzdaten bezogen sich auf freiwillige Angaben der kontrollierten Personen. Zukünftig sind die Mitarbeiter der BVG und die Fremddienstleister angewiesen, auf den Einwilligungsformularen keine Vermerke anzubringen.

4.2 Verkehr

4.2.1 Die Angst vor dem Fahrtenbuch

Ein Petent wandte sich wegen eines für ihn nicht nachvollziehbaren Informationsvorgangs zwischen dem Polizeipräsidenten von Berlin - Referat Verkehrsordnungswidrigkeiten - und dem Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) an uns. Dabei sei, so berichtete der Petent, ein Aktenvorgang mit dem Vermerk „Akte nach Kenntnisnahme bitte vernichten“ vom Polizeipräsidenten an das LABO übersandt worden. Ferner habe die Polizei Daten über mehrere geringfügige, überwiegend eingestellte und zudem länger zurückliegende Verfahren zu kleineren Verstößen im ruhenden Verkehr dem LABO unzulässigerweise übermittelt.

Wir haben die Angelegenheit beim Polizeipräsidenten und beim LABO überprüft und festgestellt, dass gegenüber dem Fahrzeughalter eine Vielzahl von Kostenbescheiden wegen Halte- und Parkverstößen aufgrund der Nichtfeststellung des verantwortlichen Fahrzeugführers vor Eintritt der Verfolgungsverjährung ergangen war. Im Zusammenhang mit einem dieser Verfahren hatte das Referat Verkehrsordnungswidrigkeiten festgestellt, dass eine auffällige Vielzahl weiterer Verfahren im ruhenden Verkehr während eines länger zurückliegenden Zeitraumes mit demselben Fahrzeug vorlag. Da bei keinem der Verkehrsverstöße der verantwortliche Fahrer rechtzeitig feststellbar war, hatte die Polizei das LABO eingeschaltet, um die Prüfung einer Fahrtenbuchanordnung nach den Vorgaben der Straßenverkehrszulassungsordnung (StVZO) einzuleiten.

Dem Ersuchen wurde eine eigens ausgedruckte Akte in Papierform beigefügt. Die Akte enthielt die Aufschrift: „Die von mir mitgesandte OWiG-Akte ist zu vernichten“. Das Referat Verkehrsordnungswidrig-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

keiten führt die Akten zu den Ordnungswidrigkeitenverfahren elektronisch. Deshalb war die Rücksendung des ausgedruckten Vorgangs, der bei der Polizei weiterhin in elektronischer Form vorlag, durch das LABO nicht erforderlich. Der Hinweis, die Akte zu vernichten, war sachlich und rechtlich deshalb nicht zu bemängeln.

Das LABO war auch rechtlich befugt, zur Prüfung der Fahrtenbuchauflage den ausgedruckten Vorgang zu verarbeiten und zu nutzen und im Rahmen dieser Aufgabenerfüllung aufzubewahren. Dies galt auch für die Hinweise auf die früheren eingestellten Bußgeldverfahren. Nach § 49 a Abs. 2 OWiG i. V. m. § 14 Abs. 1 Nr. 7 b Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) war die Datenübermittlung zumindest in diesem Fall zulässig. Denn Verwaltungsbehörden dürfen nach dieser Vorschrift von Amts wegen personenbezogene Daten aus Ordnungswidrigkeitenverfahren den zuständigen Behörden und Gerichten übermitteln, soweit dies aus der Sicht der übermittelnden Stelle für die Rücknahme, die Einschränkung oder den Widerruf einer verkehrsrechtlichen Erlaubnis des Betroffenen erforderlich ist. Der Einwand des Petenten, es habe sich nur um geringfügige Verkehrsverstöße gehandelt, widerlegt die Zulässigkeit einer solchen Datenübermittlung angesichts der Vielzahl der Ordnungswidrigkeiten nicht. Denn nach der Rechtsprechung erfordern auch geringfügige Verstöße ordnungsrechtliche Maßnahmen, wenn der Fahrerlaubnisinhaber die Rechtsvorschriften über den ruhenden Verkehr nicht anerkennt und offensichtlich nicht willens ist, auch bloße Ordnungsvorschriften, die im Interesse eines geordneten, leichten und ungefährdeten Verkehrs geschaffen sind, einzuhalten[61]. Auch das Verwaltungsgericht Berlin[62] hat eine beharrliche Missachtung von Park- und Halteverboten als Ausdruck dafür gewertet, dass der Fahrzeughalter als Verkehrsteilnehmer nicht gewillt ist, die Verkehrsregelungen zu beachten, wenn er den verantwortlichen Fahrer innerhalb der Verjährungsfrist nicht so rechtzeitig benennt, dass dieser zur Verantwortung gezogen werden kann.

Wir haben bei den uns bekannt gewordenen Vorfällen - es lagen uns mehrere Eingaben mit diesem Anliegen vor - den Informationsaustausch zwischen dem Polizeipräsidenten, Referat Verkehrsordnungswidrigkeiten, und dem LABO dann nicht bemängelt, wenn eine außergewöhnliche Häufung von Verkehrswidrigkeiten diesen Datenaustausch rechtfertigte. Allerdings haben wir das Referat Verkehrsordnungswidrigkeiten darauf hingewiesen, dass eine unbefristete Speicherung und Nutzung geringfügiger Verkehrsverstöße nicht zulässig ist. Vielmehr verlangt der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit, dass die Ange-

Der Senat sowie der Polizeipräsident in Berlin teilen in diesem Zusammenhang hinsichtlich der ungeregelten Aufbewahrungs- und Nutzungsfristen die Bedenken des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Der Polizeipräsident in Berlin hat daher dem Berliner Beauftragten für Datenschutz und Informationsfreiheit in analoger Anwendung der §§ 28 und 29 Abs. 1 Satz 1 StVG eine Frist von zwei Jahren vorgeschlagen.

Dieser Vorschlag wird zur Zeit vom Berliner Beauftragten für Datenschutz und Informationsfreiheit ge-

[61] Bundesverwaltungsgericht, Urteil v. 17. Dezember 1976 – VII C 57.75; Buchholz 442.10 § 4 StVG Nr. 49

[62] Beschluss v. 11. Juli 2006 – VG 20 a 149.06

messenheit der Speicherungs- und Nutzungsdauer zu wahren ist. Bei den uns geschilderten Vorfällen konnten wir keine unverhältnismäßige Datenspeicherung oder -nutzung feststellen, jedoch steht eine angemessene Regelung der Speicherungs- und Nutzungsfristen solcher Daten für den Zweck der Anordnung eines Fahrtenbuchs noch aus.

Die Aufbewahrungs- und Nutzungsdauer der Daten über festgestellte geringfügige Verkehrsverstöße sind so zu begrenzen, dass ein Verstoß gegen den Verhältnismäßigkeitsgrundsatz ausgeschlossen werden kann.

prüft; nach Einschätzung des dort zuständigen Bearbeiters wird man sich voraussichtlich auf diese Lösung verständigen können. Damit würde der Forderung des Berliner Beauftragten für Datenschutz und Informationsfreiheit, die Aufbewahrungs- und Nutzungsdauer der Daten über festgestellte geringfügige Verkehrsverstöße so zu begrenzen, dass ein Verstoß gegen den Verhältnismäßigkeitsgrundsatz ausgeschlossen werden kann, einvernehmlich entsprochen

4.2.2 Die *Anhörungsbogen* im Bußgeldverfahren

Einem Ordnungswidrigkeitenverfahren geht in der Regel der Versand eines Anhörungsbogens an die Beschuldigten voraus. Diese Anhörungsbogen werfen immer wieder datenschutzrechtliche Fragen auf, wie zwei Beispiele zeigen.

Statt online: „ohne Leine“

Ein Berliner Hundehalter sollte sich dafür verantworten, dass er seinen Hund unangeleint in einer geschützten Grünanlage herumlaufen ließ. Der Anhörungsbogen, den das Bezirksamt Friedrichshain-Kreuzberg von Berlin, Abteilung für Stadtentwicklung und Bauen, Ordnungsamt, dem Hundehalter zuschickte, enthielt die Aufforderung an den Hundehalter, auch seine Telefonnummer anzugeben. Während der Fragebogen den Hinweis enthielt, dass die Angaben zur Sache freiwillig und die Daten zur Person gesetzliche Pflichtangaben wären, fehlte bei der Frage nach der Telefonnummer ein solcher Hinweis.

Die Rechtsvorschrift des § 111 OWiG enthält eine abschließende Aufzählung der Daten, die im Rahmen der ordnungsrechtlichen Anhörung als Pflichtangaben vom Beschuldigten anzugeben sind. Die im Anhörungsbogen abgefragte Telefonnummer war durch § 111 OWiG nicht gedeckt, da die Angabe der Telefonnummer in § 111 OWiG nicht vorgesehen ist. Das Formular war insoweit mangelbehaftet. Es wurde nach unserem Hinweis unverzüglich korrigiert. Anhörungsbogen, bei denen nach der Telefonnummer unter der missverständlichen Rechtsbelehrung des § 111 OWiG gefragt wurde, waren auch in anderen Bezirken in Gebrauch. Aufgrund unseres Hinweises erklärten sich die uns bekannt gewordenen Bezirksämter jedoch unverzüglich einverstanden, einen Freiwilligkeitshinweis für die Angabe der Telefonnummer in den Anhörungsbogen einzufügen.

Missverständlich war ein weiteres Anhörungsformular, bei dem, abgespalten von den im Übrigen zutreffenden Freiwilligkeitshinweisen, nach dem Verursacher eines ordnungswidrigen Geschehens gefragt wurde. Da ein Beschuldigter nicht verpflichtet ist,

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

anzugeben, wen er für den Verursacher einer Ordnungswidrigkeit hält, darf diese Frage nur im Zusammenhang mit einem ausdrücklichen Hinweis auf die Freiwilligkeit gestellt werden. Etwas anderes gilt lediglich nach § 31 a Abs. 2 und 3 der Straßenverkehrszulassungsordnung (StVZO - Fahrtenbuchanordnung) für die Angabe des Kraftfahrzeugführers im Straßenverkehr, wonach der Kfz-Halter verpflichtet ist, den Fahrer, der eine zu ermittelnde Verkehrsordnungswidrigkeit begangen hat, durch Vorlage des Fahrtenbuches rechtzeitig zu benennen, wenn er nicht selbst den jeweiligen Verkehrsverstoß verursacht hatte. Bei Hundehaltern ist dies jedoch nicht vorgesehen und erscheint auch nicht als erforderlich, sind doch Hund und Herrchen oder Frauchen in der Regel unzertrennlich.

Gerade im Ordnungsrecht ist die genaue Gestaltung des Anhörungsbogens als Datenerhebungsformular dringend angezeigt. Der Anhörungsbogen ist gewissermaßen der Legitimationsausweis der Behörde für die Rechtsstaatlichkeit der Datenerhebung.

Wie sich aus der Berichtsdarstellung ergibt, sind die bezirklichen Ordnungsämter bestrebt, bei der Gestaltung der Anhörungsbogen Hinweise des Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Fehlerhaftigkeit der Anhörungsbogen zu berücksichtigen und entsprechende Berichtigungen vorzunehmen. Soweit dies im Einzelfall erforderlich sein sollte, wird die für die Ordnungsämter zuständige Leitstelle des Landesamtes für Bürger- und Ordnungsangelegenheiten bereit sein, hierbei Hilfestellung zu geben.

4.2.3 Verfahren zur Beschaffung neuer mobiler Datenerfassungsgeräte (MDE)

Das Bezirksamt Mitte von Berlin unterrichtete uns über die Beschaffung neuer mobiler Datenerfassungsgeräte und Software zur Erfassung von Ordnungswidrigkeiten für die Außendienstmitarbeiter der bezirklichen Ordnungsämter. Die vorhandenen Geräte für diese Aufgabe entsprachen weder bei Hardware noch bei Software den Anforderungen an eine zeitgemäße informationstechnisch gestützte Bearbeitung. Die alte Technik wurde bei der Errichtung der bezirklichen Ordnungsämter von der Polizei übernommen und bis heute eingesetzt.

Das Projekt, welches unter anderem vorsah, die Ausschreibung von Hardware, Software und den entsprechend ergänzenden Leistungen vorzubereiten und zu platzieren, beinhaltet die Lieferung und Inbetriebnahme von 469 Geräten zur mobilen Datenerfassung von Ordnungswidrigkeiten und zur Datenübermittlung an ein zentrales Serversystem.

Das Sicherheitskonzept, das für die Sicherstellung der Anforderungen an eine sichere Datenverarbeitung gefordert wird und auf einer Risikoanalyse aufbaut, wurde vom Informationstechnischen Dienstleistungszentrum Berlin (ITDZ) nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellt. Dies ist die Voraussetzung dafür, dass die Verantwortungsträger der Bezirksämter nachvollziehen können, ob die getroffenen Maßnahmen gegen

bestehende Risiken angemessen sind und ob Risiken bestehen, gegen die noch keine Maßnahmen ergriffen wurden. Ein solches Konzept ist sowohl für das Verfahren als auch für das Behördennetzwerk zu erstellen.

Aufbauend auf der Ermittlung der Schutzbedürftigkeit, einer Bedrohungsanalyse sowie der Risikoanalyse wurden mithilfe der Bausteine der IT-Grundschutzkataloge des BSI die für eine datenschutzgerechte Datenverarbeitung benötigten Maßnahmen ergriffen. In einer abschließenden Restrisikoanalyse wurden die nicht tragbaren Risiken durch die Anwendung spezieller Maßnahmen ausgeräumt.

Das Projekt ist ein Beispiel für die erfreulicherweise zunehmende Anzahl von IT-Einführungen, bei denen professionell erstellte Sicherheitskonzepte für Klarheit über die angemessenen Maßnahmen für den technischen und organisatorischen Datenschutz sorgen.

4.3 Justiz

4.3.1 Ein Datenschutzskandal: Verdeckte Ermittlungen gegen Unschuldige

Drei Petenten versuchten ihre spärlichen Einkünfte aufzubessern, indem sie die im Preis reduzierten Restposten einer Möbelhauskette aufkauften und im Internet versteigerten. Das Unternehmen registrierte lediglich, dass die Petenten die Waren unter dem offiziellen Einkaufspreis für Neuware veräußerten, und zeigte sie bei der Staatsanwaltschaft an. Aus der Ermittlungsakte ergab sich, dass die Staatsanwaltschaft in diesem Fall unter Missachtung offensichtlich entlastender Indizien die drei Petenten unter anderem mit einer längerfristigen Observation, einem Auskunftsverlangen über ihre Telefonverbindungsdaten und schließlich einer Telefonüberwachung überzog. Als diese letzte Maßnahme schließlich lupenrein die Unschuld der Petenten ergab, benachrichtigte die Staatsanwaltschaft jeden einzelnen von der Telefonüberwachung betroffenen Gesprächspartner der Petenten in einer Weise, die den Verdacht eines strafbaren Verhaltens der Petenten im Raum stehen ließ und überdies über deren sämtliche Telefonkontakte informierte.

Die Durchsicht der staatsanwaltlichen Ermittlungsakte ergab, dass die Staatsanwaltschaft die Anzeige des Unternehmens zunächst nicht hinterfragte, sondern in Annahme einer Bandenkriminalität unvermittelt verdeckte Ermittlungen gegen die Petenten einleitete. Bei der Observation stellten die Ermittler fest, dass einer der Petenten verpackte Ware in dem Unternehmen kaufte. Diese Tatsache und der (aus der Akte einfach erkennbare) Umstand, dass dieselbe gekaufte Warenart bereits einmal als "gestohlen" angezeigt worden war, veranlasste die Staatsanwaltschaft nicht etwa dazu, die Strafanzeige des Unternehmens zu hinterfragen. Vielmehr veranlasste sie weiter gehende ver-

Der Senat kann der Bewertung der Sachbehandlung der Staatsanwaltschaft Berlin in dem in Rede stehenden Ermittlungsverfahren durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht beipflichten, denn die Staatsanwaltschaft unterliegt zur Erfüllung ihres gesetzlichen Auftrages - der Verpflichtung zur Aufklärung und Verfolgung von Straftaten - dem Grundsatz der freien Gestaltung des Ermittlungsverfahrens.

Sie ist gehalten, zur Sachverhaltsaufklärung alle zulässigen, ihr geeignet und erforderlich erscheinenden Maßnahmen zu ergreifen. Maßgeblich hierfür ist nicht

deckte Ermittlungsmaßnahmen gegen die Petenten. Erst als die auf Antrag der Staatsanwaltschaft vom Amtsgericht angeordnete Telefonüberwachung unmissverständlich offenbarte, dass die Petenten Restposten aufkauften, lud die Staatsanwaltschaft sie vor, um ihnen Gelegenheit zu geben, den Tatverdacht endgültig auszuräumen.

Nach unserer Bewertung verletzte die Vorgehensweise der Staatsanwaltschaft in mehrfacher Hinsicht erheblich die Persönlichkeitsrechte der Petenten:

Als "Herrin" des Ermittlungsverfahrens hat die Staatsanwaltschaft die Aufgabe, bei ihren Ermittlungen nicht nur die zur Belastung, sondern auch die zur Entlastung der beschuldigten Personen dienenden Umstände zu ermitteln (vgl. § 160 Abs. 2 Strafprozessordnung – StPO). Dabei ist sie verpflichtet zu berücksichtigen, dass verdeckte Ermittlungsmaßnahmen regelmäßig erheblich in Grundrechte der überwachten Personen eingreifen. Bei solchen verdeckten Ermittlungsmaßnahmen muss die Staatsanwaltschaft daher besonders sorgfältig prüfen, ob die Ermittlungsmaßnahme zur Erforschung des Sachverhalts wirklich erforderlich ist.

Diesen Grundsatz hat die Staatsanwaltschaft offensichtlich missachtet. Bereits als die Staatsanwaltschaft ohne weitere Rückfragen bei dem Anzeigenerstatter eine längerfristige Observation einleitete, war die Erforderlichkeit der verdeckten Ermittlungsmaßnahme fraglich. Spätestens jedoch, als ein Petent dabei beobachtet wurde, wie er eine Warenart kaufte, die aktenkundig bereits kurz zuvor schon einmal versteigert worden war, hätte die Staatsanwaltschaft stutzig werden müssen: Warum kauft ein Beschuldigter eine Ware, die er dem Anzeigenerstatter zufolge zuvor immer gestohlen haben soll? Das Versteigern gekaufter neuwertiger Waren im Internet ist weder unüblich noch strafbar. Jedenfalls hätte die Staatsanwaltschaft noch einmal sorgfältig überprüfen müssen, ob weitere verdeckte Maßnahmen, die noch intensiver in das Persönlichkeitsrecht der Petenten eingriffen, wirklich notwendig waren. Dass die Unschuld der Petenten aufgrund eines Zufalls durch die eingriffsintensivste Maßnahme aufgedeckt wurde, ändert nichts an der Schädigung der Betroffenen durch die Ermittlungsmaßnahmen und rechtfertigt nicht die laxe Handhabung rechtsstaatlicher Erfordernisse.

Der Fall erhärtet auch die Vermutung, dass die Strafverfolgungsbehörden und Gerichte die Telekommunikationsüberwachung immer mehr als Routineinstrument einsetzen, ohne zuvor weniger einschneidende Maßnahmen auch nur in Betracht zu ziehen. Davon legen die jährlichen Statistiken zur Überwachung des Telefon- und E-Mail-Verkehrs ein beredtes Zeugnis ab.

Eine weitere erhebliche Verletzung der Persönlich-

der Kenntnisstand, wie er sich nach dem Abschluss der Ermittlungen darstellt, sondern derjenige im Zeitpunkt der Aufnahme der Ermittlungen. Dieser Grundsatz der freien Gestaltung des Ermittlungsverfahrens ist überdies auch bei der Ausübung der Aufsicht durch die hierfür zuständige Senatsverwaltung für Justiz zu beachten. Die hier relevanten Ermittlungen wurden durch eine schlüssige und begründete Strafanzeige der Firma IKEA, welcher umfängliche Unterlagen zu den beobachteten Vorfällen beigefügt waren, ausgelöst. Einen Anlass zu weiteren Nachfragen bei der Anzeigeerstatterin hat die Anzeige nicht geboten. Vielmehr hat die Staatsanwaltschaft Berlin zu Recht entschieden, zunächst von den weiteren strafprozessual zulässigen Ermittlungsmaßnahmen, hier der Observation nach § 163 StPO, Gebrauch zu machen. Soweit der Bericht die Überwachung der Telekommunikation rügt, weist der Senat darauf hin, dass diese Ermittlungsmaßnahme aufgrund eines richterlichen Beschlusses durchgeführt wurde und die Überprüfung richterlicher Entscheidungen in Ermittlungs- und Strafverfahren dem Berliner Beauftragten für Datenschutz und Informationsfreiheit nach § 24 Abs. 2 des Berliner Datenschutzgesetzes aufgrund der mit Verfassungsrang ausgestatteten richterlichen Unabhängigkeit verwehrt ist. Gleiches gilt, soweit die Staatsanwaltschaft Berlin aufgrund richterlichen Beschlusses die Observation der seinerzeit Beschuldigten fortgesetzt hat. Die Staatsanwaltschaft Berlin hat schließlich den Zeitraum für beide Maßnahmen nicht ausgeschöpft sondern entschieden, die Maßnahmen vorzeitig zu beenden und das Ermittlungsverfahren mangels hinreichenden Tatverdachts eingestellt. Nach dem Abschluss der Telekommunikationsüberwachungsmaßnahmen hat sie die hiervon Betroffenen entsprechend § 101 Abs. 1 StPO davon unterrichtet, dass von diesen geführte Gespräche überwacht worden sind. Soweit beanstandet wird, dass die Staatsanwaltschaft Berlin in den Benachrichtigungen nicht mitgeteilt hat, dass der Tatverdacht inzwischen ausgeräumt wurde, weist der Senat darauf hin, dass die Gesetzeslage dies nicht vorsieht. Soweit die Staatsanwaltschaft Berlin, wie weiter beanstandet, die Benachrichtigungen an jeden überwachten Gesprächsteilnehmer zu sämtlichen Telefonkontakten aller Beschuldigten gesandt hat, hätte es eines erheblichen Aufwandes unter erneuter Auswertung der Maßnahmen bedurft, um eine konkretere Zuordnung vorzunehmen. Ein Aufschieben der Benachrichtigung und im Ergebnis auch der gebotenen Löschung der Daten bis zum Vorliegen der notwendigen Auswertungsergebnisse scheint problematisch. Dennoch hält es der Senat für erforderlich zu prüfen, welche Möglichkeiten bestehen, um in künftigen vergleichbaren Fällen den daten-schutzrechtlichen Interessen Betroffener bei der Benachrichtigung über verdeckte Ermittlungsmaßnahmen insgesamt besser gerecht zu werden. Hierzu wird die zuständige Senatsverwaltung für Justiz, in welcher der Abstimmungsprozess zu der vorliegenden Beanstandung derzeit andauert, sich gesondert an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

keitsrechte der Petenten erfolgte anlässlich der Benachrichtigung der Telefongesprächspartner. Die Staatsanwaltschaft hat zwar nach § 101 StPO die Betroffenen von einer verdeckten Telefonüberwachung zu benachrichtigen. Es liegt aber auf der Hand, dass sie dabei die Grundrechte der überwachten Zielpersonen nicht missachten darf. Falls wie hier ein Tatverdacht vollständig ausgeräumt worden ist, muss die Staatsanwaltschaft dies den betroffenen Gesprächsteilnehmern auch unmissverständlich mitteilen, um so unnötigen Schaden von den unverdächtigen Beschuldigten abzuwenden. Überdies ist es offensichtlich datenschutzrechtlich nicht erforderlich, dass jeder überwachte Gesprächsteilnehmer über *sämtliche* Telefonkontaktdaten *aller* Beschuldigten informiert wird, obwohl er beispielsweise nur mit einem Beschuldigten auf einem Telefonanschluss telefoniert hat.

Die Staatsanwaltschaft hat ihre Vorgehensweise im Wesentlichen verteidigt und die Auffassung vertreten, die Ermittlungsmaßnahmen seien rechtmäßig gewesen. Die Erforderlichkeit der Maßnahmen sei zum Zeitpunkt der jeweiligen Anordnung und nach der Strafanzeige zu beurteilen gewesen. Die danach notwendige Observation habe keine Hinweise zur Herkunft der Waren erbracht. Dementsprechend sei die Telekommunikationsüberwachung nach damaligem Wissenstand die einzige Möglichkeit gewesen, die Herkunft der Ware zu ermitteln. Der Umstand, dass den Kommunikationspartnern der Petenten die Anschlüsse aller drei Petenten genannt worden seien statt nur der Anschluss, auf dem tatsächlich telefoniert wor-den sei, erklärte die Staatsanwaltschaft damit, dass genau diese Information in der von ihr zur Benachrichtigung der Betroffenen angeforderten Aufstellung der Polizei gefehlt habe.

Der Generalstaatsanwalt hat sich dieser Stellungnahme angeschlossen und überdies bezweifelt, ob die Kontrollkompetenz des Berliner Beauftragten für Datenschutz auch die Kontrolle der staatsanwaltlichen Ermittlungsentscheidungen mit umfasse. Die Kontrolle dieser Entscheidungen durch den Berliner Beauftragten für den Datenschutz sei durch die Strafprozessordnung ausgeschlossen, für die Prüfung sowohl der Annahme des Anfangsverdachts als auch der Beachtung des Subsidiaritätsprinzips sei kein Raum.

Die Darlegungen der Staatsanwaltschaft sind nicht nachzuvollziehen. Das gilt zunächst für die Kontrollkompetenz. Die Annahme des Generalstaatsanwalts, dass die Strafprozessordnung es dem Berliner Beauftragten für Datenschutz und Informationsfreiheit verwehre, Entscheidungen der Staatsanwaltschaft auf ihre Rechtmäßigkeit zu überprüfen, ist rechtswidrig. Die Staatsanwaltschaft ist eine öffentliche Stelle des Landes Berlin, die bei der Anwendung der Strafprozessordnung auch der Kontrolle durch den Berliner Be-

auftragten für Datenschutz und Informationsfreiheit unterliegt. Dieser kontrolliert im Land Berlin die Einhaltung des Berliner Datenschutzgesetzes sowie „anderer Vorschriften“ über den Datenschutz (§ 24 Abs. 1 Satz 1 BlnDSG). Die Strafprozessordnung ist eine solche „andere Vorschrift“. Das Bundesverfassungsgericht hat den Datenschutzbeauftragten die Aufgabe zugewiesen, für den *vorbeugenden Grundrechtsschutz* beim Umgang mit personenbezogenen Daten zu sorgen. Dies gilt auch für das Strafverfahren. Selbst wenn bestimmte Ermittlungsmaßnahmen (z. B. Observation, Telefonüberwachung) von einem Gericht angeordnet werden, das insoweit nicht der Kontrolle durch den Datenschutzbeauftragten unterliegt, stellt dies die Staatsanwaltschaft, die diese Anordnungen beantragt hat, nicht von der Datenschutzkontrolle frei.

Was die Notwendigkeit der Ermittlungsmaßnahmen anbelangt, ändern die Hinweise der Staatsanwaltschaft nichts an dem Umstand, dass spätestens die Observation nicht zu übersehende Hinweise auf die Unschuld der Petenten ergab, die von der Staatsanwaltschaft offenbar nicht berücksichtigt wurden.

Wir haben deshalb die Vorgehensweise als erheblichen Datenschutzverstoß beanstandet.

Verdeckte Ermittlungen greifen stets erheblich in die Grundrechte der Betroffenen ein. Auch wenn der beschriebene Vorgang in seiner krassen Missachtung von Datenschutzrechten sicherlich einen Ausnahmefall darstellt, verdeutlicht er jedoch zugleich die Risiken, die für den normalen, rechtstreuen Bürger mit einer stetigen Ausweitung von gesetzlichen Ermittlungsbefugnissen bei gleichzeitigem Abbau von rechtsstaatlich begründeten Tatbestandsvoraussetzungen einhergehen. Der Gesetzgeber sollte vor der Schaffung von verdeckten Ermittlungsbefugnissen deshalb auch diese Risiken beachten. Die Staatsanwaltschaft hat vor der Veranlassung verdeckter Ermittlungsmaßnahmen besonders sorgfältig zu prüfen, ob diese Maßnahmen tatsächlich für die Sachverhaltsaufklärung erforderlich sind. Bei der gesetzlich vorgeschriebenen *Benachrichtigung* Dritter über Telefonüberwachungsmaßnahmen nach Einstellung des Verfahrens muss sie auch darüber informieren, dass der Beschuldigte entlastet ist.

4.3.2 Namensbezogene Ankündigung von Anklagen gegenüber dem Landgericht

Ein Rechtsanwalt wies uns darauf hin, dass die Staatsanwaltschaft regelmäßig Listen der Strafverfahren an das Präsidium des Landgerichts versendet, in denen in nächster Zeit Anklage erhoben wird und bei denen mit einer Hauptverhandlungsdauer von mindestens drei Tagen zu rechnen ist. Die Listen enthielten bislang neben dem Aktenzeichen auch die Nachnamen der jeweils Beschuldigten sowie den Tatvorwurf.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Der Generalstaatsanwalt hat hierzu dargelegt, dass das Landgericht auf diese Listen angewiesen sei, um die Geschäftsverteilung auf den zu erwartenden Geschäftsanfall einzustellen. Nur mit dieser Vorabinformation könne die gemäß Art. 6 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK) rechtsstaatlich gebotene zügige Bearbeitung umfangreicher Verfahren sichergestellt werden. Aus Sicht des Generalstaatsanwalts steht auch die Vorschrift des § 170 Abs. 1 Strafprozessordnung (StPO), der eine Übermittlung der Anklageschrift an das zuständige Gericht erst bei der Erhebung der öffentlichen Klage vorsieht, einer derartigen Unterrichtung nicht entgegen. Diese sei vielmehr nach § 474 Abs. 1 StPO zulässig.

Die Übersendung von Listen mit den Nachnamen der Beschuldigten an das Landgericht ist mangels Rechtsgrundlage datenschutzrechtlich jedoch nicht zulässig. Die StPO berechtigt nicht zu der Mitteilung, dass gegen bestimmte Personen wegen bestimmter Delikte *demnächst* Anklage erhoben werden wird. Eine derartige Datenübermittlung kann nicht auf § 474 Abs. 1 StPO gestützt werden. Nach dieser Vorschrift erhalten Justizbehörden Akteneinsicht für Zwecke der Rechtspflege, d. h. für ein bestimmtes anderes Verfahren oder einen bestimmten anderen Vorgang und damit für einen Zweck, der nicht der Grund der Erhebung der Informationen im Ursprungsverfahren war. Die Vorschrift regelt die Informationsübermittlung für verfahrensexterne Zwecke und erfasst daher die hier infrage stehende Unterrichtung durch die Staatsanwaltschaft gerade nicht.

Unabhängig davon ist eine Verarbeitung personenbezogener Daten nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der Daten verarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Zur Erreichung des Zwecks der Verfahrensbeschleunigung ist eine Weitergabe der Namen der Beschuldigten aber gerade nicht erforderlich, da seit Januar 2006 auch beim Landgericht Berlin eine von Buchstaben unabhängige Geschäftsverteilung im Turnusverfahren gilt. Ausreichend ist insoweit die Übermittlung des Aktenzeichens des Verfahrens, der zu erwartenden Anzahl der Beschuldigten, des Tatvorwurfs sowie der voraussichtlichen Verhandlungsdauer.

Das Verfahren wurde unseren Vorgaben entsprechend umgestellt. Seit April 2006 wird auf die Übermittlung von Namen der Beschuldigten verzichtet.

4.3.3 Strafanträge wegen dienstlich nicht veranlasster Datenabrufe

Nach dem Berliner Datenschutzgesetz sind wir befugt, wegen gesetzlich bestimmter rechtswidriger Datenverarbeitungsvorgänge gegen den jeweils Verantwortlichen Strafantrag zu stellen. Anders als einige andere

Behörden Berlins macht der Polizeipräsident in Berlin von der Gelegenheit Gebrauch, bei datenschutzrechtswidrigem Handeln seiner Beamtinnen und Beamten das öffentliche Interesse an der Strafverfolgung durch uns überprüfen zu lassen.

Wie in den vergangenen Jahren legten uns der Polizeipräsident in Berlin und die Staatsanwaltschaft auch in dem Jahr 2006 regelmäßig Ermittlungsakten vor, um uns die Prüfung zu ermöglichen, ob wir einen Strafantrag nach dem Berliner Datenschutzgesetz für geboten halten. In allen 15 Fällen hatten Polizeibeamte ohne dienstliche Veranlassung Daten aus polizeilichen Informationssystemen abgerufen. In etwa der Hälfte der zu entscheidenden Fälle bejahten wir ein öffentliches Interesse an der Strafverfolgung, in den übrigen Fällen stellten wir keinen Strafantrag.

Wesentliche Kriterien für die Bejahung eines öffentlichen Interesses an der Strafverfolgung bildeten in dem Berichtsjahr vor allem etwaige Folgen einer rechtswidrigen Datenabfrage für die Geschädigten oder die Anzahl der Abrufe durch den oder die Beschuldigten. Selbst bei einem einzigen Datenabruf stellten wir regelmäßig einen Strafantrag, wenn er offenkundig mit der Absicht getätigt wurde, um die geschädigten Personen aufzusuchen und weiter gehend zu schädigen (z. B. durch Beleidigungen und Körperverletzungen). Ein vergleichbares öffentliches Interesse an der Strafverfolgung sahen wir bei Datenabrufen als gegeben an, die auf eine Weiterleitung von personenbezogenen Daten Unverdächtiger an das kriminelle Milieu abzielten. Strafanträge wurden auch gestellt, wenn Beamte die polizeilichen Informationssysteme ohne dienstliche Veranlassung häufig nutzten.

Insgesamt entspricht es unserer Erfahrung, die auch durch unsere Prüfpraxis bestätigt wird, dass die Berliner Polizei strafbaren Datenschutzverstößen in den eigenen Reihen regelmäßig konsequent nachgeht, wenn sie hiervon erfährt. Es gibt zu denken, dass keine andere große Behörde in Berlin uns in entsprechender Weise gebeten hat, die Stellung von Strafanträgen zu prüfen.

Der professionelle Umgang der Berliner Polizei und Staatsanwaltschaft mit dienstlich nicht veranlassten Datenabrufen durch Polizeibeamte ist derzeit als vorbildlich zu bewerten.

4.3.4 Weitergabe von vertraulichen Informationen an Dritte durch die *Justizvollzugsanstalt* Tegel

Es wandte sich ein Haftinsasse an uns, der ein als vertraulich gekennzeichnetes Schreiben an die Abteilung Sicherheit der Justizvollzugsanstalt gerichtet hatte. Der Brief enthielt u. a. Informationen über den anstaltsinternen Drogenhandel. Das Schreiben sei an einen Mitarbeiter des Vollzugsmanagements gelangt, der es, ohne den Namen des Petenten zu schwärzen, in

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ein Verfahren vor der Strafvollstreckungskammer gegen einen Mithäftling eingebracht habe. Der von dem Verfahren vor der Strafvollstreckungskammer betroffene Gefangene habe auf diese Weise Kenntnis von dem Schreiben erlangt und daraufhin in der Justizvollzugsanstalt verbreitet, dass der Petent ein „Informant“ sei. Dies habe zu massiven Bedrohungen des Petenten durch Mitgefangene geführt.

Auf unsere Bitte um Stellungnahme hat die Justizvollzugsanstalt den Sachverhalt im Wesentlichen bestätigt und dazu die Auffassung vertreten, dass die Strafvollstreckungskammer den Sachverhalt umfassend zu ermitteln habe. Die Vollzugsbehörde sei verpflichtet, gegenüber dem Gericht die Grundlagen ihrer angefochtenen Entscheidung vollständig darzulegen. Der Aspekt der Drogenabhängigkeit und der daraus resultierenden Verstrickungen des Petenten in den anstaltsinternen Drogenhandel sei für die Beurteilung der Authentizität des Schreibens erforderlich gewesen. Im Rahmen des rechtlichen Gehörs sei dem Antragsteller in dem Verfahren offenbar die Stellungnahme der Anstalt mit den dazugehörigen Anlagen übersandt worden. Ob die besagten Informationen eine Bedrohungssituation für den Petenten hervorgerufen hätten, sei nicht zu verifizieren.

Wir haben diese Datenweitergabe an die Strafvollstreckungskammer als datenschutzrechtlichen Mangel kritisiert. Auf entsprechende Mitteilung an die Senatsverwaltung für Justiz hat diese die Rechtsauffassung der Justizvollzugsanstalt Tegel verteidigt. Sie hat die Auffassung vertreten, dass die Datenweitergabe im Rahmen des gerichtlichen Rechtsschutzverfahrens zulässig gewesen sei. Nach dem Strafvollzugsgesetz sei eine Verarbeitung personenbezogener Daten unabhängig von dem ursprünglichen Erhebungszweck zulässig, wenn sie dem gerichtlichen Rechtsschutz diene. Demgemäß umfasse die einschlägige Vorschrift auch personenbezogene Äußerungen der Vollzugsbehörde gegenüber der Strafvollstreckungskammer, die für das gerichtliche Verfahren erforderlich seien. Das sachliche Erfordernis der Datenweitergabe habe die Justizvollzugsanstalt sachlich zutreffend dargelegt.

Diese Ausführungen sind für uns nicht nachvollziehbar. Für eine Offenlegung des Absenders eines Beschwerdeschreibens gegenüber dem Gericht bestand erkennbar kein Bedarf. Die Strafvollzugssache betraf die Frage der Rechtmäßigkeit der Anordnung einer Postkontrolle gegen einen anderen Strafgefangenen sowie die Aushändigung zweier in dessen Haftraum beschlagnahmter Schreiben. Hierfür war es nicht erforderlich, die Rolle des Petenten in anderen Zusammenhängen gegenüber der Strafvollstreckungskammer offen zu legen. Die Person des Petenten spielte für die Entscheidung offensichtlich keine Rolle.

Die Strafvollstreckungskammer hat ausweislich der uns vorliegenden Informationen das Schreiben des Pe-

Der Senat teilt aus den im Bericht des Beauftragten für Datenschutz und Informationsfreiheit bereits ausführlich dargelegten Gründen die Rechtsauffassung sowohl der Justizvollzugsanstalt Tegel als auch der Senatsverwaltung für Justiz, dass die Datenweitergabe im Rahmen des gerichtlichen Rechtsschutzverfahrens vor der Strafvollstreckungskammer des Landgerichts Berlin zulässig gewesen ist.

Eine Offenlegung des Absenders des Beschwerdeschreibens gegenüber der Strafvollstreckungskammer ist für das Gerichtsverfahren erforderlich gewesen, da Streitgegenstand des gerichtlichen Verfahrens die Rechtmäßigkeit der Anordnung einer Postkontrolle und der Beschlagnahme von Schreiben des Vereins „Humanitas-Human Aid“ gegen einen anderen Strafgefangenen, §§ 28 Abs. 2 Nr. 2, 19 Abs. 2 i.V.m. 70 Abs. 2 Nr. 2 Strafvollzugsgesetz war, und nur durch die Offenlegung des Namens der Beweis der Rechtmäßigkeit der Postkontrolle und der Beschlagnahme dahingehend zu führen gewesen ist, dass der Verein, dessen 1. Vorsitzender der Petent zum damaligen Zeitpunkt war, erheblich die Sicherheit und Ordnung in der Justizvollzugsanstalt Tegel gestört und gegen die Anstaltsordnung verstoßen hat (vgl. Beschluss des Landgerichts Berlin vom 4. Oktober 2005 – 543 StVK (Vollz) 476/05).

tenten auch nicht ausdrücklich angefordert. Vielmehr hat die Justizvollzugsanstalt dieses Schreiben von sich aus dem Gericht übergeben. Überdies wäre es ausreichend gewesen, wenn die Justizvollzugsanstalt ein vollständig anonymisiertes Schreiben an die Kammer übersandt hätte. Über eine spätere Deanonymisierung hätte bei konkretem Bedarf und nach Anforderung durch das Gericht entschieden werden können.

Die Preisgabe des Namens des Petenten hat zumindest nach seiner Darlegung zur erheblichen Beeinträchtigung seiner Persönlichkeitsrechte geführt.

Auch wenn Justizvollzugsanstalten Stellungnahmen vor Vollstreckungskammern abgeben, müssen sie im Rahmen der Erforderlichkeitsprüfung die Auswirkungen von Datenübermittlungen an das Gericht für betroffene Gefangene berücksichtigen. Eine Weitergabe von „Informantennamen“ kommt daher nur in Betracht, wenn dies für das Gerichtsverfahren notwendig ist.

4.3.5 Juristische *Staatsprüfung*: Im Krankheitsfall nur mit Diagnosedaten Vergünstigungen?

Ein Petent beschwerte sich bei uns darüber, dass er anlässlich der Verlängerung einer Prüfungsfrist wegen schwerer Erkrankung dem Gemeinsamen Juristischen Prüfungsamt der Länder Berlin und Brandenburg (GJPA) ein ärztliches Attest vorgelegt habe, das dort nicht für ausreichend befunden worden sei. Das GJPA verlange unter anderem Angaben zur genauen Diagnose, welche Beschwerden aufgetreten seien und in welchem Umfang und bei welchen Ärzten der Petent in Behandlung gewesen sei.

Wir haben die Eingabe zum Anlass genommen, generell eine Klärung herbeizuführen, welche Daten das GJPA erhebt, wenn Prüflinge unter Berufung auf Krankheitsfälle Vergünstigungen bei Prüfungen beantragen.

Das GJPA machte im Hinblick auf die Eingabe zunächst geltend, gemäß der verwaltungsgerichtlichen Rechtsprechung sei der Prüfling verpflichtet, aktiv bei der Klärung der Frage mitzuwirken, ob ihm Vergünstigungen gewährt werden könnten. Daraus ergebe sich seine Obliegenheit, ein hinreichend aussagekräftiges Attest und damit regelmäßig auch die Mitteilung der Diagnose vorzulegen.

Wir haben demgegenüber darauf abgestellt, dass die Angabe einer Diagnose im vorgelegten Attest nur in den Einzelfällen verlangt werden könne, in denen die rechtlichen Voraussetzungen einer Meldefristverlängerung nicht ohne Vorliegen einer Diagnose geklärt werden könnten. Insoweit sei eine routinemäßige Abfrage der ärztlichen Diagnose unzulässig.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Nach klärenden Gesprächen sind wir mit dem GJPA zu einer übereinstimmenden Rechtsauffassung gelangt, die sinngemäß unter anderem folgende Punkte enthält:

1. Im Zusammenhang mit einem Antrag auf Meldefristverlängerung (wie bei dem Petenten) gilt, dass die Angabe einer Diagnose im vorgelegten Attest nur in den Einzelfällen verlangt werden kann, in denen die rechtlichen Voraussetzungen einer Meldefristverlängerung nicht ohne Vorliegen einer Diagnose geklärt werden können.

   Einem amtsärztlichen Attest kommt dabei ein höherer Beweiswert zu als einem privatärztlichen Attest. In Bezug auf Letzteres können daher strengere Anforderungen an die Substantiierung des Krankheitsbildes gestellt werden.

   Legt der Antragsteller ein nicht aussagekräftiges Attest vor, so weist ihn das GJPA zunächst nur auf das Erfordernis eines substantiierten Attestes hin. Falls dieses nicht vorgelegt wird oder falls seine Angaben Zweifel an den rechtlichen Voraussetzungen für eine Meldefristverlängerung nicht ausräumen, kann das Prüfungsamt allerdings in Einzelfällen auch die Angabe einer Diagnose verlangen.

2. Begehrt ein Prüfling unter Berufung auf eine Erkrankung Vergünstigungen im Rahmen der Prüfung (Verlängerung der Bearbeitungszeit oder ähnliche Vergünstigungen), so hat er im Rahmen seiner Mitwirkungspflicht ein Attest vorzulegen, das eine Beurteilung durch das GJPA erlaubt, ob die Voraussetzungen für die begehrte Begünstigung vorliegen. Das Attest muss also hinreichend aussagekräftig sein, damit das GJPA die geltend gemachte krankheitsbedingte Prüfungsunfähigkeit bzw. die krankheitsbedingten Einschränkungen beurteilen kann. Hierfür ist regelmäßig eine Beschreibung der Symptome erforderlich. Eine konkrete Diagnose kann darüber hinaus erforderlich sein, um insbesondere festzustellen, dass die Prüfungsunfähigkeit bzw. eingeschränkte Prüfungsfähigkeit nicht auf eine chronische Erkrankung zurückzuführen oder ausschließlich anlagebedingt ist. In einem solchen Fall könnte nämlich nach dem Prüfungsrecht keine Vergünstigung erteilt werden. Zweifel gehen insoweit zulasten des Prüflings.

Das GJPA hat angekündigt, den genauen Wortlaut der gemeinsam getroffenen Feststellungen zur Rechtslage auf seiner Website zu veröffentlichen.

Finanzen

4.4.1 Was steht in meiner *Steuerakte*?

Ein Petent begehrte beim Finanzamt die Einsichtnah-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

me in seine eigene Steuerakte. Sein Antrag auf Akteneinsicht wurde vom Finanz-amt mit der Begründung abgelehnt, dass die Abgabenordnung (AO) im Gegensatz zu § 29 Verwaltungs-verfahrensgesetz (VwVfG) kein Akteneinsichtsrecht gewähren würde.

Tatsächlich ist weder in § 91 AO noch an anderer Stelle in der Abgabenordnung das Recht des Beteiligten auf Akteneinsicht normiert. Dennoch kann die Finanzbehörde den Beteiligten am Steuerverfahren im Einzelfall nach Ermessen eine derartige Akteneinsicht gewähren (vgl. AEAO zu § 91 AO). Ob das Finanzamt im Fall des Petenten von diesem Ermessensspielraum Gebrauch gemacht hat bzw. welche Gründe im Rahmen der Ermessensentscheidung zur Ablehnung seines Antrages auf Akteneinsicht geführt haben, ließ sich dem Ablehnungsbescheid nicht entnehmen. Die Senatsverwaltung für Finanzen vertrat dazu die Auffassung, dass es sich hier nicht um eine datenschutzrechtliche, sondern um eine Frage der Fachaufsicht handeln würde. Der Betroffene habe die Möglichkeit, die von der AO vorgesehene Wahrung des Rechtsschutzes im Rahmen des außergerichtlichen Rechtsbehelfs durchzusetzen. Von dieser Möglichkeit habe der Petent Gebrauch gemacht, indem er dem Ablehnungsbescheid widersprochen habe. Die in der angefochtenen Ablehnung der Akteneinsicht fehlende Begründung bzw. Ermessensdarlegung könne grundsätzlich in der Einspruchsentscheidung nachgeholt und so ein etwaiger Begründungsmangel geheilt werden. Das Finanzamt werde dies bei seiner Einspruchsbearbeitung berücksichtigen.

Unabhängig von den Regelungen in der AO steht den Betroffenen auch ein Auskunfts- bzw. Einsichtsrecht nach § 16 Berliner Datenschutzgesetz (BlnDSG) zu. Dies wird von der Senatsverwaltung für Finanzen jedoch vehement bestritten. Sie vertritt dazu die irrige Auffassung, dass das Berliner Datenschutzgesetz im Bereich der AO generell nicht anwendbar bzw., dass es „verfassungskonform“ im Sinne der AO auszulegen sei. Unsere langjährigen Versuche, hier zu einer Annäherung der Rechtspositionen zu gelangen, waren bisher vergeblich. Es ist nicht ersichtlich, dass die Senatsverwaltung für Finanzen ihre Auffassung in diesem Punkt ändern und den Betroffenen zukünftig die ihnen zustehenden weiter gehenden Rechte auf Akteneinsicht einräumen wird. Auch der Bundesgesetzgeber hat es bisher versäumt, die Abgabenordnung zumindest klarstellend um Datenschutzrechte der Steuerschuldner zu ergänzen. Das ist alles andere als „verfassungskonform“.

Entgegen der Auffassung der Senatsverwaltung für Finanzen können Steuerpflichtige unter den Voraussetzungen des § 16 BlnDSG Einsicht in bzw. Auskunft aus ihren Steuerunterlagen erhalten.

Es ist höchstrichterlich geklärt (BFH vom 4. Juni 2003, VII B 138/01), dass der fehlende Anspruch auf Akteneinsicht im außergerichtlichen Besteuerungsverfahren und eine insoweit der Finanzverwaltung eingeräumte Ermessensausübung nicht gegen verfassungsrechtliche Grundsätze verstoßen und die AO eine abschließende Regelung für den Umgang mit den im Besteuerungs-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

verfahren gespeicherten Daten enthält. Die insoweit einschränkenden bereichsspezifischen Regelungen in Steuerangelegenheiten gehen dem BDSG und entsprechenden landesrechtlichen Datenschutzgesetzen vor.
Die Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit lässt diese höchstrichterlich bestätigten Rechtsgrundsätze außer Acht und widerspricht zudem Art. 31 GG.

4.4.2 Der Gast als relevantes Steuerdatum – Informanten- und Quellenschutz bei Journalisten

Ein Journalist, der Bewirtungskosten, die anlässlich von Gesprächen mit Informanten entstanden waren, als abzugsfähige Werbungskosten in seiner Einkommensteuererklärung angegeben hatte, wurde vom Finanzamt darauf hingewiesen, dass er die Veranlassung der betrieblichen Aufwendungen unter schriftlicher Angabe von Ort, Tag, Teilnehmern und Anlass der Bewirtung darzulegen habe. Bei Bewirtung in einer Gaststätte habe er neben der Rechnung auch Angaben zum Anlass und zu den Teilnehmern der Bewirtung zu machen, wobei letztere namentlich benannt werden müssten. Der Journalist war – unter Berufung auf den journalistischen Quellenschutz – nicht bereit, dem Finanzamt die Namen seiner Recherchequellen zu offenbaren.

Das Finanzamt ist nach § 10 Abs. 1 i. V. m. § 6 Abs. 1 BlnDSG berechtigt, personenbezogene Daten beim Betroffenen zu erheben, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat. Eine solche Rechtsvorschrift ist § 4 Abs. 5 Satz 1 Nr. 2 Einkommensteuergesetz (EStG). Danach dürfen Aufwendungen für die Bewirtung von Personen aus geschäftlichem Anlass den Gewinn nicht mindern, soweit sie 70 % der Aufwendungen überschreiten, die nach der allgemeinen Verkehrsauffassung als angemessen anzusehen und deren Höhe und betriebliche Veranlassung nachgewiesen sind. Zum Nachweis hat der Steuerpflichtige schriftlich Angaben über den Ort, Tag, die Teilnehmer und den Anlass der Bewirtung sowie die Höhe der Aufwendungen zu machen. Hat die Bewirtung in einer Gaststätte stattgefunden, so genügen nach § 4 Abs. 5 Nr. 2 Satz 3 EStG Angaben zu dem Anlass und den Teilnehmern der Bewirtung.

Ein Journalist kann diese Angaben nach ständiger Rechtsprechung[63] nicht unter Berufung auf das Pressegeheimnis (Art. 5 Abs. 1 Satz 2 GG) oder das Auskunftsverweigerungsrecht nach § 102 Abs. 1 Nr. 4 AO 1977 verweigern.

Das Grundrecht der *Pressefreiheit* aus Art. 5 Abs. 1 Satz 2 GG umfasst den gesamten Prozess der Informationsermittlung. Durch die Pflicht zur Angabe der Namen von Informanten ist ein Journalist mithin in

[63] Bundesfinanzhof, Urteil v. 15. Januar 1998 – 8 IV R 81/96, BStBl. II 1998, 263

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

seinem Grundrecht aus Art. 5 Abs. 1 Satz 2 GG betroffen. Allerdings ist das Grundrecht der Pressefreiheit nicht schrankenlos. Es steht vielmehr unter dem Vorbehalt der allgemeinen Gesetze (Art. 5 Abs. 2 GG). Die Abzugsregelung des § 4 EStG ist Teil eines derartigen allgemeinen Gesetzes. Sie zielt nicht auf die Einschränkung der Pressefreiheit als solche ab, sondern soll das von der Rechtsordnung anerkannte Gut der Besteuerungsgleichheit sicherstellen. Dem steuerlichen Gleichbehandlungsgebot und damit dem öffentlichen Interesse an der Sicherung des Steueraufkommens ist im Ergebnis der Vorrang vor dem Pressegeheimnis einzuräumen.

Sofern sich ein Journalist auf sein schützenswertes, für seinen Beruf schlechthin konstituierendes Interesse an der Geheimhaltung seiner informatorischen Quellen beruft, hat der Bundesfinanzhof ausgeführt, dass eben dieses Geheimhaltungsinteresse des Steuerpflichtigen in § 30 AO berücksichtigt wird. Nach § 30 AO sind Amtsträger verpflichtet, das Steuergeheimnis zu wahren. § 30 AO dient also sowohl dem privaten Geheimhaltungsinteresse des Steuerpflichtigen als auch dem des Informanten. Durch den normierten Grundsatz der Amtsverschwiegenheit werden die mit dem privaten Geheimhaltungsinteresse kollidierenden, weitgehenden Offenbarungspflichten des Steuerpflichtigen zwar nicht aufgehoben oder eingeschränkt – jedoch wird durch § 30 AO den Folgen der Offenbarungspflicht entgegengetreten. Auch wenn der betroffene Journalist also die Namen seiner Informanten in der Steuererklärung angibt, gibt er die Namen seiner Informanten nicht in der Weise preis, dass diese „nach außen“ dringen. Im Ergebnis bleiben die Namen der breiten Öffentlichkeit in dem Sinne verborgen, als dass diese nicht jedem beliebigen Dritten zur Verfügung stehen. Bei der Güterabwägung ist darüber hinaus zu berücksichtigen, dass das Steuergeheimnis gemäß § 30 AO, § 355 StGB mit empfindlicher Strafe bewehrt ist.

Nach Auffassung des Bundesfinanzhofs besteht hier auch kein Auskunftsverweigerungsrecht zum Schutz bestimmter Berufsgeheimnisse nach § 102 Abs. 1 Nr. 4 AO. Journalisten können danach zwar Auskünfte über die Person des Verfassers, Einsenders oder Gewährsmanns von Beiträgen und Unterlagen sowie über die ihnen im Hinblick auf ihre Tätigkeit gemachten Mitteilungen verweigern. Dies gilt allerdings nur dann, wenn es sich um Beiträge für den redaktionellen Teil ihrer Arbeit handelt. Davon ist jedoch nach Auffassung des Gerichts bei Hintergrund- und Informationsgesprächen mit Informanten nicht auszugehen. Da nach § 102 Abs. 1 Nr. 4 2. Halbsatz AO die Vorschrift des § 160 AO unberührt bleibt und Journalisten deshalb selbst bei Zahlung von Bestechungs- oder sog. Schmiergeldern die Namen der Empfänger offenbaren müssen, scheidet eine Verweigerung der nach § 4 Abs. 5 Satz 1 Nr. 2 S. 1 EStG geforderten Angaben zu

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Teilnehmern und Anlass einer Bewirtung unter Berufung auf das Pressegeheimnis erst recht aus[64].

Bei der Geltendmachung von Bewirtungskosten als abzugsfähige Werbungskosten im Rahmen der Einkommensteuererklärung hat der Steuerpflichtige zum Nachweis schriftlich Angaben über den Ort, Tag, die Teilnehmer und den Anlass der Bewirtung sowie die Höhe der Aufwendungen zu machen. Hat die Bewirtung in einer Gaststätte stattgefunden, so genügen nach § 4 Abs. 5 Nr. 2 Satz 3 EStG Angaben zu dem Anlass und den Teilnehmern der Bewirtung. Diese Nachweispflicht gilt grundsätzlich auch für Journalisten, sofern sie Bewirtungskosten, die anlässlich von Gesprächen mit Informanten entstanden waren, geltend machen.

Diese Auffassung ist zutreffend.

4.4.3 Auskunftsverweigerungsrecht von Ärzten

Infolge der Änderung in der Rechtsprechung zur Umsatzsteuer im Jahre 2001 ist die Erstellung von ärztlichen Gutachten nur noch dann steuerbefreit, wenn therapeutische Ziele verfolgt werden. Dabei entsteht die Frage, ob das Finanzamt im Rahmen einer Betriebsprüfung in einer Arztpraxis Einblick in die Patientenakten und die entsprechenden ärztlichen Gutachten verlangen kann.

Steuerpflichtige, die eine Steuerbefreiung für sich in Anspruch nehmen wollen, haben im Rahmen ihrer Mitwirkungspflichten grundsätzlich die Beweislast für das Vorliegen der Voraussetzungen gegenüber den Finanzbehörden zu tragen. Da es im vorliegenden Fall entscheidend auf die Art der ärztlichen Gutachtertätigkeit ankommt, hat der steuerpflichtige Arzt den Finanzbehörden in Zweifelsfällen die erforderlichen Auskünfte zu geben bzw. Unterlagen vorzulegen, die die Behörde in die Lage versetzen, den Steuertatbestand zu prüfen.

Dem steht entgegen, dass Ärzte nach § 102 Abs. 1 Nr. 3 c AO die Auskunft darüber verweigern können, was ihnen in dieser Eigenschaft anvertraut oder bekannt geworden ist. Bei einem ärztlichen Gutachten ist (unabhängig davon, ob es der Umsatzsteuerbefreiung unterliegt oder nicht) grundsätzlich davon auszugehen, dass es medizinische patientenbezogene Daten enthält, die dem besonderen Schutz des § 102 AO unterliegen. Dies gilt auch für den Patientennamen, der dem Arzt als Bestandteil der ärztlichen Behandlung oder zur Erstellung des Gutachtens in seiner Eigenschaft als Arzt zur Kenntnis gelangt ist. Da der Name des Patienten unmittelbar mit der in einem Gutachten enthaltenen Anamnese und Diagnose sowie den ärztlichen Schlussfolgerungen verbunden ist, unterliegt er der *ärztlichen Schweigepflicht*, deren Bruch nach § 203 Abs. 1 Nr. 3 StGB strafbar ist.

[64] Urteil des Bundesfinanzhofs v. 15. Januar 1998 – 8 IV R 81/96, BStBl. II 1998, 263

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Um die Mitwirkungspflichten der Ärzte in eigenen Steuerangelegenheiten nicht durch die §§ 102 und 104 AO zu beschränken, hat der Bundesfinanzhof[65] entschieden, dass Ärzte ggf. Auszüge bzw. Zusammenstellungen aus ihren Gutachten zu fertigen und vorzulegen haben, die sich auf die finanziellen Beziehungen beschränken und die keine Tatsachen enthalten, welche ein Auskunfts- und Vorlageverweigerungsrecht begründen.

In dem zitierten Beschluss des Bundesfinanzhofs vom 11.12.1957, BStBl 1958 III S. 86 billigt dieser jedoch dem Finanzamt zu, dass dieses, „wenn es berechtigte Zweifel an der Richtigkeit und Ordnungsmäßigkeit der Buchführung des Arztes hat, diesem aufgeben kann, in geeigneter Form Auszüge und Zusammenstellungen über die einzelnen Besuche und sonstigen Leistungen aus der Patientenkartei mit Namensangaben für die Nachprüfung zu fertigen, welche sich auf die finanziellen Beziehungen beschränken und welche die das Auskunftsverweigerungsrecht begründenden Tatsachen nicht enthalten. Dabei ist das Auskunftsverlangen des Finanzamtes wie bei allen Ermessensentscheidungen an die Grundsätze von Recht und Billigkeit gebunden."

Vor dem Hintergrund dieser Rechtsprechung des Bundesfinanzhofs haben wir der Senatsverwaltung für Finanzen empfohlen, bei Betriebsprüfungen in Berliner Arztpraxen wie folgt zu verfahren:

Der steuerpflichtige Arzt hat anlässlich einer Betriebsprüfung in Zweifelsfällen Kopien der erforderlichen Unterlagen zu fertigen und den Finanzbehörden vorzulegen. In den kopierten Unterlagen hat er sämtliche Angaben, die nicht zur Aufgabenerfüllung des Finanzamtes erforderlich sind, (z. B. durch Schwärzung) unkenntlich zu machen. Dies betrifft insbesondere Angaben über Erkrankungen, Anamnesen, Diagnosen und ärztliche Schlussfolgerungen aber auch den Patientennamen. Dabei handelt es sich um die Gesundheitsdaten eines Dritten (des Patienten), deren Erhebung in keinem Fall für die Feststellung des steuerrelevanten Sachverhaltes im Rahmen einer Betriebsprüfung in einer Arztpraxis erforderlich ist.

Die Erstellung eines ärztlichen Gutachtens ist nach § 4 Nr. 14 UStG nur dann steuerfrei, wenn ein therapeutisches Ziel im Vordergrund steht. Die Schwärzung der Angaben über Erkrankungen, Anamnesen, Diagnosen und ärztlichen Schlussfolgerungen hätte zur Folge, dass das Finanzamt nicht über die Umsatzsteuerbefreiung entscheiden könnte.

Eine Verbindung dieser umsatzsteuerlich relevanten Angaben mit dem Namen des Patienten ist nicht erforderlich. Zur Beurteilung, ob die Umsatzsteuerfreiheit für Leistungen gewährt werden kann, genügt eine Anonymisierung (z.B. mit Fall 1, Fall 2 usw.).

Der Patientenname ist ein besonderes medizinisches Datum, das der ärztlichen Schweigepflicht unterliegt. Entsprechende Auskunftsbegehren der Finanzbehörden im Rahmen einer Betriebsprüfung kann der Arzt nach § 102 Abs. 1 Nr. 3 c AO verweigern.

Bei berechtigten Zweifeln an der Richtigkeit und Ordnungsmäßigkeit der Buchführung des Arztes ist nach der Rechtsprechung des Bundesfinanzhofs (s.o.) das Finanzamt berechtigt, ein entsprechendes Auskunftsbegehren unter Beachtung der Grundsätze von Recht und Billigkeit zu stellen.

5 Sozialordnung

5.1 Soziales

5.1.1 Verschärfungen beim „Arbeitslosengeld II"

Über die Vielzahl der mit der praktischen Umsetzung des Sozialgesetzbuches Zweites Buch (SGB II) verbundenen Datenschutzprobleme haben wir in der Vergangenheit ausführlich berichtet[66]. Bedauerlicherweise hat sich auch zwei Jahre nach Inkrafttreten der Arbeitsmarktreform an den Problemen nicht viel verän-

[65] BStBl. III 1958, 86

[66] JB 2004, 3.1; JB 2005, 3.2

dert. Die im Zusammenhang mit „Hartz IV“ stehenden Beschwerden machen weiterhin einen wesentlichen Anteil der an uns gerichteten Eingaben aus.

Wir haben die häufigsten an uns herangetragenen Fraugen gemeinsam mit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg in einem gemeinsamen „Ratgeber zu Hartz IV“ zusammengestellt. Der Ratgeber ist auf unserer Homepage unter http://www.datenschutzberlin.de/infomat/dateien/ratgeber/Ratgeber HartzIVStand13.11.06.pdf veröffentlicht und kann dort abgerufen oder bei uns kostenlos angefordert werden. Wir gehen davon aus, dass wir den Betroffenen damit eine wertvolle Hilfe für den Umgang mit den Jobcentern an die Hand geben.

Zum 1. August 2006 sind mit dem Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende[67] zahlreiche Änderungen der sog. Hartz-IV-Gesetze in Kraft getreten, die aus datenschutzrechtlicher Sicht für die Betroffenen weitere Verschlechterungen mit sich bringen. Die Bundesregierung hat mit dem Gesetz in erster Linie das Ziel verfolgt, die stark gestiegenen Kosten der Hartz-IV-Reform zu begrenzen. Zu diesem Zweck wurden in größter Eile Instrumente zur noch intensiveren Überwachung der Hartz-IV-Empfänger geschaffen, um vermuteten Leistungsmissbrauch einzudämmen und auf diese Weise die gewünschten Einsparungen zu erreichen. Hierbei werden die Betroffenen pauschal unter Generalverdacht gestellt, ohne dass verlässliche Zahlen über tatsächlichen Leistungsmissbrauch vorliegen. Vielmehr deutet alles darauf hin, dass die Kosten der Hartz-IV-Reform, also der Geltendmachung bestehender Rechtsansprüche, deutlich unterschätzt worden sind. Im Einzelnen greifen aus unserer Sicht insbesondere folgende Änderungen in gravierender Weise in das Recht auf informationelle Selbstbestimmung der Betroffenen ein:

Lebt eine Person mit einem Hilfebedürftigen in einem gemeinsamen Haushalt so zusammen, dass nach verständiger Würdigung der gemeinsame Wille anzunehmen ist, Verantwortung füreinander zu tragen und füreinander einzustehen, gehört dieser zur sog. *Bedarfsgemeinschaft*. Während bislang das Jobcenter im Rahmen seiner Pflicht zur Ermittlung des Sachverhaltes das Bestehen einer nichtehelichen Lebensgemeinschaft nachzuweisen hatte, enthält das Gesetz nunmehr eine Auflistung von Kriterien, nach denen eine Vermutung für eine nichteheliche Lebensgemeinschaft besteht. Als Beispiele hierfür sind ein länger als ein Jahr andauerndes Zusammenleben oder das Zusammenleben mit einem gemeinsamen Kind zu nennen. Treffen diese Kriterien bei einem Betroffenen zu, hat dieser nachzuweisen, dass eine eheähnliche Gemeinschaft nicht besteht. Mit der Neuregelung wird

[67] BGBl. I, 1706.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

die Beweislast dem Betroffenen auferlegt, der nunmehr selbst darzulegen und zu beweisen hat, dass er nicht in einer nichtehelichen Lebensgemeinschaft lebt.

Gegen diese Neuregelung bestehen erhebliche datenschutzrechtliche Bedenken. Für die Betroffenen beispielsweise in einer Wohngemeinschaft wird es nämlich oftmals nicht zu vermeiden sein, ihre Leistungsbedürftigkeit Dritten zu offenbaren, um gegenüber dem Jobcenter nachzuweisen, dass eine nichteheliche Lebensgemeinschaft nicht besteht. Darüber hinaus werden sie sogar verpflichtet, Auskunft über die Lebensverhältnisse unbeteiligter Dritter zu geben, die nach dem Sozialgesetzbuch gar nicht zur Mitwirkung verpflichtet wären.

Das Sozialgesetzbuch – Zweites Buch (SGB II) enthielt bislang bereits eine Befugnis zur Überprüfung der Leistungsbezieher im Wege des automatisierten Datenabgleichs. Durch das Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende wurden die Möglichkeiten zum Datenabgleich erweitert. Nunmehr ist eine flächendeckende Überprüfung aller Leistungsbezieher ohne Vorliegen von Verdachtsmomenten in kurzen Zeiträumen von drei Monaten vorgesehen. Auch wurden die Möglichkeiten zum Datenabgleich zum Zweck der Bekämpfung von Leistungsmissbrauch erweitert. So ist es zulässig, Auskünfte beim Kraftfahrtbundesamt zur Überprüfung von Kraftfahrzeughalterdaten einzuholen, um z. B. die Angemessenheit des genutzten Kraftfahrzeuges beurteilen zu können. Des Weiteren dürfen Auskünfte aus dem Melde- und dem Ausländerzentralregister eingeholt werden.

Die Neuregelungen widersprechen dem Grundsatz der Verhältnismäßigkeit. Belege für das tatsächliche Vorliegen nennenswerter Missbrauchsfälle fehlen, in denen z. B. das genutzte Kraftfahrzeug als nicht angemessen anzusehen wäre. Vor diesem Hintergrund ist es äußerst zweifelhaft, ob eine derartige Ausweitung der Möglichkeiten zum Datenabgleich überhaupt erforderlich ist, um Leistungsmissbrauch zu verhindern, oder ob es hierfür nicht weniger einschneidende Mittel gegeben hätte. Es wird in das Grundrecht auf informationelle Selbstbestimmung einer ganzen Gruppe eingegriffen, ohne dass die dem Gesetz zugrunde gelegte Annahme, diese Eingriffe seien durch eine erhebliche Anzahl von Fällen des Leistungsmissbrauchs gerechtfertigt, durch konkrete Zahlen belegt worden wäre.

Nach gemeinsamer Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und der Landesbeauftragten für den Datenschutz handelt es sich bei den Arbeitsgemeinschaften, d. h. in Berlin den Jobcentern, um eigenverantwortlich Daten verarbeitende Stellen, die der Kontrolle der Landesbe-

auftragten für den Datenschutz unterliegen[68]. Allerdings hat es der Gesetzgeber versäumt, gesetzlich klarzustellen, dass die Datenschutzkontrolle in den Arbeitsgemeinschaften, d. h. in Berlin den Jobcentern, von den Landesbeauftragten für den Datenschutz ausgeübt wird, und damit für die nötige Rechtsklarheit zu sorgen.

Nach wie vor gilt es eine Reihe datenschutzrechtlicher Fragen beim „Arbeitslosengeld II“ endgültig zu klären. Die Datenschutzbeauftragten des Bundes und der Länder werden sich weiterhin dafür einsetzen, dass die Situation Betroffener nicht durch Gesetzesänderungen weiter verschlechtert wird.

5.1.2 Einführung des *Fallmanagements* in der Eingliederungshilfe

Mit Inkrafttreten des Sozialgesetzbuches Zwölftes Buch - Sozialhilfe (SGB XII) zum 1. Januar 2005 haben sich die Aufgaben der Sozialhilfeträger wesentlich verändert. Die weit überwiegende Mehrheit der erwerbsfähigen ehemaligen Empfänger von Leistungen nach dem Bundessozialhilfegesetz (BSHG) wird nunmehr von den Jobcentern betreut und bezieht Leistungen nach dem SGB II. Die Sozialämter in den Bezirken betreuen dagegen im Wesentlichen kranke, behinderte und pflegebedürftige Personen, die nicht erwerbsfähig sind und bei denen es daher in der Regel auch nicht um die Eingliederung in den Arbeitsmarkt geht. Vielmehr versteht die Berliner Sozialverwaltung die nach dem SGB XII definierte Aufgabe der Beratung, Unterstützung und Aktivierung der Leistungsberechtigten dahingehend, diesen Menschen ein möglichst selbst bestimmtes Leben in eigener Verantwortung zu ermöglichen.

Der Berliner Senat hat entschieden, im Leistungsbereich der Eingliederungshilfe für Menschen mit Behinderung ab 2006 das sog. Fallmanagement einzuführen. Damit wird das Ziel verfolgt, die herkömmliche Sachbearbeitung, die in erster Linie die Aufgabe hatte, über Kostenübernahmen zu entscheiden, durch eine neue Qualität der Betreuung zu ersetzen. Der Fallmanager hat neben der reinen Kostenträgerschaft die Aufgabe, das Eingliederungshilfeverfahren für den Leistungsberechtigten zu planen, zu dokumentieren und über den Bewilligungszeitraum bedarfsgerecht anzupassen. Als ein wesentliches Element des Fallmanagements soll das in § 58 SGB XII vorgesehene Instrument des *Gesamtplans* zum Einsatz kommen. Die Vorschrift sieht vor, dass der Leistungsträger bei der Aufstellung des Gesamtplans und der Durchführung der Leistungen mit dem behinderten Menschen und den sonst im Einzelfall Beteiligten, u. a. dem Ge-

[68] JB 2005, 3.2, S. 42; Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 16./17. März 2006 „Keine kontrollfreien Räume bei der Leistung von ALG II“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 12

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

sundheitsamt, zusammenwirkt.

Die Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz hat ein Formular eines Gesamtplans für die Eingliederungshilfe volljähriger Menschen mit geistig-körperlicher Behinderung entwikkelt, das den Fallmanagern in den Bezirken einheitlich zur Verfügung stehen soll. Gleichzeitig wurde ein Formular für ein Gutachten entwickelt, mit dem angesichts der mit dem Fallmanagement verbundenen ämterübergreifenden Kommunikation zwischen den Sozialhilfeträgern und den Gesundheitsämtern das Begutachtungsverfahren weitgehend standardisiert werden soll. Beide Formulare wurden uns von der Senatsverwaltung zur datenschutzrechtlichen Bewertung vorgelegt.

Die berlinweite Einführung des Fallmanagements birgt eine Reihe grundsätzlicher datenschutzrechtlicher Probleme. Dieses hat sich bereits durch eine Vielzahl von Anfragen aus den Bezirken gezeigt, in denen schon Fallmanager tätig sind. Bei der bisherigen Trennung der Aufgaben hatte der Sozialhilfeträger im Wesentlichen über die Kostenträgerschaft zu entscheiden, während die Gesundheitsämter die medizinische bzw. psychologische Begutachtung der Betroffenen vorzunehmen und die Leistungsträger über das Ergebnis zu informieren hatten. Durch den nunmehr gewählten ganzheitlichen Ansatz der Betreuung durch den Fallmanager und einer damit verbundenen intensiveren Zusammenarbeit mit den Gesundheitsämtern benötigt der Fallmanager mehr Informationen über den Betroffenen, als dies bisher der Fall war.

Datenschutzrechtlich allerdings bemisst sich die Zulässigkeit der Datenverarbeitung an dem Kriterium der Erforderlichkeit für die Gewährung der Leistung. Der Gesetzgeber hat dem Fallmanager keine über die allgemein im Sozialdatenschutzrecht geltenden Regelungen hinausgehenden Datenverarbeitungsbefugnisse eingeräumt. Demgegenüber ist die Senatsverwaltung zunächst davon ausgegangen, den vom Fallmanager gemeinsam mit dem Betroffenen erstellten Gesamtplan vollständig dem Gutachter im Gesundheitsamt für dessen Begutachtung übergeben zu können. Diese Verfahrensweise haben wir kritisiert, da die Erforderlichkeit einer Weitergabe des vollständigen Gesamtplans für uns nicht ersichtlich war. Überdies sollte es vermieden werden, dass in unterschiedlichen Stellen Datensammlungen angelegt werden, die weder für die Leistungsgewährung noch für die medizinische Begutachtung erforderlich sind. Die Senatsverwaltung nahm daraufhin von der geplanten Verfahrensweise Abstand, den Gesamtplan an den Gutachter weiterzugeben. In Gesprächen mit der Senatsverwaltung konnte im Übrigen eine weitere Verschlankung des Formulars erreicht werden. Einige nicht erforderliche Angaben werden nunmehr ausdrücklich als freiwillige Angaben gekennzeichnet (z. B. Angaben zur Religionszugehörigkeit bzw. zu Begleiterkrankungen).

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Das Formular für die Anforderung eines vom Gesundheitsamt zu erstellenden Gutachtens durch den Fallmanager wurde zwischen der Senatsverwaltung und uns ebenfalls diskutiert. Auch hier konnte von uns eine Verschlankung des Formulars erreicht werden. Ob das Gesundheitsamt die der Behinderung zugrunde liegende Diagnose an den Fallmanager im Sozialamt weitergeben kann, ist noch nicht abschließend geklärt, aus unserer Sicht aber für den Regelfall zu verneinen. Auch vor dem Hintergrund, dass dem Fallmanager die Entscheidung darüber obliegt, welche Eingliederungsleistungen zu erbringen sind, sehen wir die Kenntnis der ärztlichen Diagnose hierfür grundsätzlich als nicht erforderlich an. Eine ärztliche Diagnose nennt nicht die Symptome einer Krankheit, sondern ist vielmehr das Ergebnis der Zuordnung der Symptome zu einer Krankheit. Aufgrund des fehlenden ärztlichen Sachverstandes des Fallmanagers ist es für diesen erforderlich, die aus der Krankheit resultierenden Beschwerden und Einschränkungen zu kennen, nicht jedoch die Diagnose.

Wir haben daher die Auffassung vertreten, die für den Fallmanager relevanten Informationen ließen sich der „Internationalen Klassifikation der Funktionsfähigkeit, Behinderung und Gesundheit (ICF)“ der WHO entnehmen. Diese Angaben sind ihm zugänglich zu machen. Eine Übermittlung der Diagnosen nach der „Internationalen statistischen Klassifikation der Krankheiten und verwandten Gesundheitsprobleme“, d. h. der sog. ICD-10-Klassifikation, erscheint dagegen nicht erforderlich. Da in dieser Frage zwischen der Senatsverwaltung und uns bislang noch keine einvernehmliche Lösung erreicht werden konnte, führen wir weitere Gespräche.

Die Einführung des Fallmanagements bringt zulasten der Betroffenen eine Reihe datenschutzrechtlicher Veränderungen mit sich. Die bisherige strikte Trennung zwischen Kostenträger und Gesundheitsamt wird mit der Folge einer umfangreicheren Datenübermittlung zwischen den Beteiligten aufgehoben. Wir sind bestrebt, die neu eingeführten Verfahrensweisen in der Form datenschutzgerecht zu gestalten, dass den Persönlichkeitsrechten der Betroffenen Rechnung getragen wird. Es ist dabei als Erfolg anzusehen, dass die ursprünglich von der Senatsverwaltung entwickelten Vordrucke des Gesamtplans sowie des Gutachtens verschlankt und in ihrem Umfang reduziert werden konnten. Die Standardisierung des Verfahrens der Gewährung einer Eingliederungshilfe bringt datenschutzrechtliche Verbesserungen mit sich, da es mit den gezielt vorgegebenen Fragen vermieden werden kann, dass umfangreiche Gutachten erstellt werden, die nicht relevante personenbezogene Daten des Betroffenen enthalten.

Die zuständige Senatsverwaltung strebt in den Gesprächen mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit eine einvernehmliche Lösung an, die mit der kurz vor der Verabschiedung stehenden und mit den kommunalen Spitzenverbänden abgestimmten vorläufigen Orientierungshilfe zur Feststellung einer wesentlichen Behinderung nach dem SGB XII der Bundesarbeitsgemeinschaft der überörtlichen Träger der Sozialhilfe vereinbar ist.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

5.1.3 Deutsche Vergangenheit und ein Literatur-Nobelpreisträger

Wenige Tage vor dem deutschen Angriff auf Polen wurde am 26. August 1939 die „Wehrmachtsauskunftsstelle für Kriegsverluste und Kriegsgefangene (WASt)" eingerichtet. Sie war eine Dienststelle des Oberkommandos der Wehrmacht und diente vorrangig der Erfassung der Verluste der deutschen Wehrmacht (Verwundungen, Erkrankungen, Sterbefälle, Vermisstenfälle).

Allein wenn man den riesigen Raum der Zentralkartei der heutigen „Deutschen Dienststelle (WASt) für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen deutschen Wehrmacht" mit seinen dort gelagerten ca. 20 Millionen Karteikarten betrachtet, bekommt man einen Eindruck von dem millionenfachen Tod und Leid, den dieser Krieg zur Folge hatte. Regal für Regal, Karton für Karton je 600 Karteikarten. Aber gleichzeitig Informationen über 600 Schicksale und Verweise auf verbliebene Unterlagen, die bei der Deutschen Dienststelle oder anderen Einrichtungen vorhanden oder leider auch nicht vorhanden sind. Die Deutsche Dienststelle verwaltet mit dieser Kartei über 4.000 Tonnen Akten und Karteimaterial. Datenschutzrechtlich sind dies zumeist personenbezogene Daten. Daher hat das Abgeordnetenhaus von Berlin im Jahre 1993 ein Gesetz über die Verarbeitung personenbezogener Daten bei der WASt verabschiedet[69]. Die konkrete Umsetzung dieses Gesetzes erfolgte durch die Verordnung über die Verarbeitung personenbezogener Daten bei der Deutschen Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen deutschen Wehrmacht.

Die heutigen Aufgaben der Deutschen Dienststelle sind vielfältig. Zu viele Schicksale sind noch ungeklärt, auch wenn derzeit in größerem Umfang Unterlagen aus Nachfolgestaaten der ehemaligen Sowjetunion eingehen und aufbereitet werden müssen. Immer wieder sind es Fragen, wie „Wo war mein Angehöriger eingesetzt?" oder „Was hat er in dieser Zeit gemacht?", „Wo ist er gefallen?" und auch eine immer häufiger gestellte Frage „Wer ist, wer war mein Vater?". Tausende von Kindern, die von ehemaligen Wehrmachtsangehörigen im In- und Ausland gezeugt wurden, wollen heute, selbst schon über 60-jährig, endlich auch von diesem Teil ihrer Wurzeln etwas erfahren. Bei jeder Anfrage hat die Deutsche Dienststelle zu prüfen, ob sie berechtigt ist, personenbezogene Daten an den Anfragenden zu übermitteln[70]. Datenschutzrechtlich einfache Fälle werden zuneh-

[69] zum Hintergrund JB 1993, 1.2

[70] schon JB 1995, 5.10 und 1998, 4.4.3

mend seltener, da zumeist nur noch die damals jüngsten Kriegsteilnehmer der Jahrgänge bis 1930, wenn sie oder ihre nächsten Angehörigen noch leben, aktiv ihre Einwilligung geben können.

Mit der Leitung der Deutschen Dienststelle haben wir verschiedene Problemkonstellationen beraten und Leitlinien zu ihrer Bewältigung entwickelt. Die Deutsche Dienststelle ist keine Einrichtung, die dem allgemeinen *Archivrecht* unterliegt. Damit sind auch für die wissenschaftliche Forschung oder historische Aufarbeitung gewisse Grenzen gesetzt. Gleichwohl sind auch hier Auskünfte oder Akteneinsicht bei Einhaltung bestimmter Regelungen und entsprechender Verpflichtungen möglich. Gegenwärtig prüfen der Bund und das Land Berlin, ob die Unterlagen der WASt in das Bundesarchiv überführt werden sollen.

Entsprechendes gilt für das bei dem Landesamt für Gesundheit und Soziales angesiedelte Krankenbuchlager. Es handelt sich hierbei um die zentrale deutsche Sammelstelle für die Krankenunterlagen aus beiden Weltkriegen (*Lazarett-Krankenbücher*) sowie für die Versorgungsunterlagen der damaligen Reichsversorgungsdienststellen, die ursprünglich auch in der Deutschen Dienststelle aufbewahrt wurden. Die Unterlagen dienen in erster Linie der Klärung von Versorgungsansprüchen oder von Vermisstenfällen.

Die breite Öffentlichkeit wurde im Berichtszeitraum auf die Deutsche Dienststelle und das Krankenbuchlager aufmerksam, nachdem sich der Schriftsteller Günter Grass öffentlich zu seiner Mitgliedschaft bei der Waffen-SS in der Endphase des Zweiten Weltkriegs bekannt hatte. Auf Anfragen von Journalisten hatten Mitarbeiter der WASt und des Krankenbuchlagers bestätigt, dass in beiden Archiven Unterlagen über den Literatur-Nobelpreisträger vorhanden seien, ohne zuvor dessen Einwilligung eingeholt zu haben. Dies war unzulässig. Weder das Informationsfreiheitsgesetz noch das Berliner Pressegesetz rechtfertigten dieses Vorgehen. Die Offenbarung von Informationen aus der WASt oder dem Krankenbuchlager an Dritte für Zwecke der zeitgeschichtlichen Forschung kommt erst in Betracht, wenn die betroffene Person eingewilligt hat oder seit mindestens zehn Jahren verstorben ist. Nachdem der Schriftsteller Einsicht in die zu seiner Person vorhandenen Unterlagen genommen hatte, stimmte er der Herausgabe an die Journalisten zu.

Als Konsequenz aus diesem Vorfall hat der Präsident des Landesamtes für Gesundheit und Soziales in Abstimmung mit uns eine Anweisung über die Offenbarung von Informationen aus dem Krankenbuchlager erlassen.

Datenschutzrechtliche Kernaufgabe der Deutschen Dienststelle und des Krankenbuchlagers bleibt die Schicksalsklärung der Vermissten oder Verschollenen für familiäre und versorgungsrechtliche Zwecke. Für

Zwecke der zeitgeschichtlichen Forschung dürfen die dort lagernden Unterlagen nur mit Einwilligung der Betroffenen oder frühestens zehn Jahre nach deren Tod genutzt werden.

5.1.4 Terroristenjagd im *Jobcenter*

Die Presse berichtete über einen Mann mit arabischem Namen, dessen Arbeitslosengeld-II-Leistungen von einem Berliner Jobcenter eingestellt wurden. Erst nach geraumer Zeit stellte sich heraus, dass er mit einer Person verwechselt worden war, deren Name auf einer im Internet veröffentlichten Liste der Vereinten Nationen stand, mit deren Hilfe seit dem 11. September 2001 die Finanzierung des Terrorismus unterbunden werden soll.

Der Sicherheitsrat der Vereinten Nationen hat unmittelbar nach den Anschlägen vom 11. September beschlossen, die Namen von terroristischen Organisationen und Einzelpersonen, die als Terroristen gelten, weltweit zu veröffentlichen. Alle Banken, Versicherungen und andere Unternehmen sind verpflichtet, sämtliche Zahlungsempfänger, Mitarbeiter und Geschäftspartner mit dieser ständig aktualisierten Liste (Embargo-Liste) abzugleichen und vorhandene Guthaben und Vermögenswerte einzufrieren. Diese Listen sind im Internet für jedermann abrufbar[71]. Damit soll die Finanzierung terroristischer Aktivitäten unterbunden werden. Die Europäische Union hat diese Sanktionen durch Verordnungen umgesetzt, die in den Mitgliedstaaten unmittelbar geltendes Recht sind[72]. Die UN-Listen werden dabei ungeprüft übernommen. In der Bundesrepublik sind die Bundesbank für die Kreditinstitute und das Bundesaufsichtsamt für das Versicherungswesen für Versicherer zentral zuständig für das Einfrieren von Geldern. Den Datenabgleich mit den Listen haben aber alle Banken im Zahlungsverkehr durchzuführen.

Rechtsschutz gegen die Aufnahme in die *UN-Embargoliste* (die von der Europäischen Union unverändert übernommen wird) gibt es nur beim Sanktionsausschuss der Vereinten Nationen. Die Rechtmäßigkeit der EG-Verordnungen ist vom Europäischen Gericht erster Instanz bestätigt worden. Dieses Gericht hat allerdings in einer Entscheidung vom Dezember 2006 erstmals die Aufnahme einer Organisation in die Liste ohne Gewährung rechtlichen Gehörs als rechtswidrig bezeichnet[73].

Nachdem wir das Jobcenter um Stellungnahme zu den Presseberichten über den arabischen Arbeitslosengeld-

[71] z. B. unter www.bundesbank.de

[72] VO (EG) Nr. 2580/2001 des Rates v. 27. Dezember 2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete Maßnahmen zur Bekämpfung des Terrorismus, ABl. EG L 344/70; VO (EG) Nr. 881/2002 des Rates v. 27. Mai 2002, ABl. EG L 139/9. Der Rat hat die Embargoliste seitdem mehrfach aktualisiert.

[73] Urteil v. 12. Dezember 2006 – Rs. T-228/02

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

II-Empfänger gebeten hatten, teilte dieses uns mit, es sei in der Angelegenheit nicht zuständig und verwies auf die Bundesbank. Erst nach Einschaltung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit konnten wir ermitteln, dass die Postbank bei der Abwicklung der Überweisungen von Arbeitslosengeld II den Abgleich mit der Antiterror-Liste durchführt. Die Postbank vertrat zunächst die unzutreffende Auffassung, sie handele im Auftrag der Bundesagentur für Arbeit. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen als für die Postbank zuständige Aufsichtsbehörde hat demgegenüber festgestellt, dass die Postbank (ebenso wie jedes andere durch die EU-Verordnungen verpflichtete Kreditinstitut) den Abgleich im eigenen Interesse durchführt und deshalb selbst datenschutzrechtlich verantwortlich ist. Aufgrund der unmittelbar bindenden Wirkung des Gemeinschaftsrechts war das Vorgehen der Postbank nicht zu beanstanden.

Allerdings haben die Datenschutzbeauftragten des Bundes und der Länder das Verfahren der Listenaufstellung zur Terrorbekämpfung als empfindlichen Eingriff in das informationelle Selbstbestimmungsrecht bezeichnet[74]; die Listen führen aufgrund spärlicher Zusatzinformationen und unsicherer Identifikation der aufgeführten Personen immer wieder zu Verwechselungen mit Unverdächtigen, die – wie der geschilderte Fall zeigt – existenzielle Folgen für die Betroffenen haben können. Die Datenschutzbeauftragten haben die Bundesregierung aufgefordert, bei den Vereinten Nationen und der Europäischen Union auf die Einhaltung rechtsstaatlicher Standards wie des rechtlichen Gehörs, eines gesicherten Identitätsnachweises und eines effektiven Rechtsschutzes zu dringen.

Schon die prinzipielle Eignung derartiger *Antiterror-Listen* zur Austrocknung der Finanzierung terroristischer Aktivitäten ist zweifelhaft. Vollends grotesk ist aber die Überprüfung von Sozialleistungsempfängern anhand der international publizierten Listen. Das gilt umso mehr, als die maßgebliche EU-Verordnung selbst vorsieht, dass die Verwendung eingefrorener Gelder zur Deckung der Grundbedürfnisse eines Terroristen z. B. für Lebensmittel, Arzneimittel oder Arzthonorare von der zuständigen nationalen Behörde genehmigt werden kann. Diese Genehmigung muss aber gesondert beantragt werden[75].

Der Abgleich mit den von den Vereinten Nationen aufgestellten Antiterror-Listen ist deutschen Banken und Versicherungen zwar durch Verordnungen des Europäischen Rates verbindlich vorgeschrieben. Das Verfahren der Aufstellung und der bisher unzureichende Rechtsschutz gegen die massiven Eingriffe in

[74] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 16./17. März 2006, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 11

[75] Art. 5 Abs. 2 und 3 der VO (EG) Nr. 2580/2001 v. 27. Dezember 2001

das informationelle Selbstbestimmungsrecht Unverdächtiger widersprechen aber Grundregeln des Rechtsstaats. Solange dieser Widerspruch nicht behoben ist, müssen die Kreditinstitute verstärkte Anstrengungen unternehmen, um Personenverwechselungen gerade bei Sozialleistungsempfängern binnen kürzester Frist aufzuklären.

5.2 Gesundheit

5.2.1 Warum sagt mir keiner was? – Das Recht auf Einsicht in die *Patientenakte*

Im vergangenen Jahr haben wir vermehrt Anfragen von Bürgern erhalten, die ihre ärztlichen Behandlungsunterlagen einsehen wollten. Einige Ärzte und Krankenhäuser lehnten diesen Wunsch ohne nähere Begründung ab oder stellten nur eine beschränkte Einsicht in Aussicht. Wir nehmen dies zum Anlass, die Rechtslage kurz darzustellen und einige praktische Hinweise zum Verfahren der Akteneinsicht zu geben.

Jeder Patient hat grundsätzlich das Recht, Einsicht in die ihn betreffende ärztliche Behandlungsdokumentation mit den Angaben zu Anamnese, Diagnose und Therapie zu nehmen. Das Einsichtsrecht als besondere Form der Auskunftserteilung folgt bereits aus dem Recht auf Selbstbestimmung und der personalen Würde des Patienten[76]. Es besteht aber auch als Nebenrecht aus dem Behandlungsvertrag und zivilrechtlich zur Durchsetzung von Rechtsansprüchen (§ 810 Bürgerliches Gesetzbuch). Ausdrücklich findet es sich schließlich in den Berufsordnungen der Ärztekammern und Zahnärztekammern wieder (vgl. § 10 Abs. 2 der Berufsordnung der Ärztekammer Berlin).

Die Art und Weise der Einsichtsgewährung (Ort, Zeitpunkt, Umstände) liegt im Ermessen des Arztes. In der Regel erfolgt die Einsicht in den Behandlungsräumen. Angemessen ist, wenn der Patient die Einsicht innerhalb eines Monats erhält. Während einer aktuellen Behandlung sollte ein mündlicher Antrag auf Einsicht ausreichend sein. Liegt die Behandlung länger zurück, sollte der Antrag schriftlich gestellt werden. Im Antrag sollte benannt werden, zu welchem Behandlungsfall Einsicht begehrt wird und welche Daten oder Unterlagen davon umfasst werden sollen.

Möglich ist statt der Einsicht in die Originalakte aber auch das Anfordern von Kopien (oder Ausdrucken) aus der Dokumentation. Es besteht zwar kein Anspruch auf Zusendung solcher Kopien, aber darauf, dass diese bei dem Arzt oder im Krankenhaus bereitgehalten werden. Der Arzt ist verpflichtet, auf Antrag die Kopien oder Ausdrucke zu fertigen, herauszugeben und zu versichern, dass die herausgegebenen Unterlagen vollständig sind. Hierfür muss der Patient

[76] BVerfG, NJW 1999, 1777

eventuell entstehende Kosten erstatten.

Die *Akteneinsicht* verfehlt ihre Informationsfunktion, wenn die Patientendaten auf eine Art und Weise festgehalten werden, die der Patient nicht versteht. Dem Arzt obliegt es daher im Rahmen von Treu und Glauben, Lesbarkeit und Nachvollziehbarkeit für die Patienten herzustellen. Die inhaltliche Vermittlung kann auch in einem Gespräch mit dem Arzt erfolgen.

Das Einsichtsrecht kann auch in der Form wahrgenommen werden, dass ein Arzt oder eine Person des Vertrauens des Patienten mit der Einsicht beauftragt wird. So kann der Patient die Herausgabe von Krankenunterlagen an den nachbehandelnden Arzt verlangen.

Das Recht auf Einsicht in die Patientendokumentation besteht, ohne dass dafür ein besonderes Interesse erklärt oder nachgewiesen werden müsste. Informationelles und medizinisches Selbstbestimmungsrecht begründen für sich schon den Anspruch, umfassend über Untersuchung und Behandlung informiert zu werden. Das Einsichtsrecht erstreckt sich nach der Rechtsprechung des Bundesgerichtshofs und dem ärztlichen Berufsrecht allerdings nur auf naturwissenschaftlich objektivierbare physische Befunde und Berichte über Behandlungsmaßnahmen, nicht hingegen auf den Teil der Dokumentation, der rein subjektive Eindrücke und Wahrnehmungen des Arztes enthält. Dies bedeutet, dass im Einzelfall die Einsicht in vorläufige Verdachtsdiagnosen verweigert werden kann, wenn die schützenswerten Interessen des Arztes das Informationsinteresse des Patienten überwiegen. Das Datenschutzrecht kennt eine solche Einschränkung im Übrigen nicht. Da die datenschutzrechtlichen Ansprüche unabhängig vom Standes- und Vertragsrecht gelten, kann bei deren Geltendmachung eine Offenlegung nicht verhindert werden, es sei denn, die subjektiven Aufzeichnungen werden zugleich durch ausdrücklich geregelte Ausnahmeregelungen abgedeckt.

Besonderheiten gelten in Bezug auf psychiatrische Behandlungen. Dort kommt der Entscheidung des Arztes, ob eine Aushändigung der Unterlagen an den Patienten medizinisch zu verantworten ist, besonderes Gewicht zu. Allerdings darf auch nach einer psychiatrischen Behandlung die Herausgabe der Patientenunterlagen nicht pauschal unter Hinweis auf ärztliche Bedenken verweigert werden. Die entgegenstehenden therapeutischen Gründe sind vielmehr nach Art und Richtung näher zu kennzeichnen. Der Arzt hat sich bei seiner Entscheidung einerseits an dem aus dem Persönlichkeitsrecht abgeleiteten Anspruch des Patienten auf Wissen um die Diagnose und die Behandlung, andererseits aber auch an medizinisch begründeten Patientenschutzinteressen zu orientieren. Solche Schutzinteressen sind insbesondere gegeben, wenn infolge der Einsicht in die gesamte Behandlungsakte eine schwere Selbstgefährdung des Patienten droht.

Darüber hinaus kann er auch Interessen Dritter, die in die Behandlung einbezogen worden sind, sowie eigene Interessen an der Erhaltung der therapeutischen Handlungsfähigkeit mit berücksichtigen. Bei noch nicht abgeschlossener Behandlung kann eine Verweigerung daher eher begründet werden als in den Fällen, in denen die Behandlung bereits seit Jahren beendet ist oder abgebrochen wurde.

Stirbt der Patient, so geht das Einsichtsrecht hinsichtlich der Krankenunterlagen, soweit vermögensrechtliche Komponenten betroffen sind, auf die Erben über. Die Einsichtnahme darf aber nicht dem ausdrücklich geäußerten oder mutmaßlichen Willen des Verstorbenen widersprechen. Darüber hinaus steht auch den nächsten Angehörigen ein Einsichtsrecht zu, das sich bereits aus den nachwirkenden Persönlichkeitsbelangen des Verstorbenen herleitet. Es ist gegen die Interessen des Arztes an der über den Tod hinaus fortwirkenden Verschwiegenheitspflicht abzuwägen.

Das Recht auf Akteneinsicht zählt zu den zentralen Datenschutzrechten der Patienten. Es ist Grundlage für die Kenntnis des eigenen Gesundheitszustandes und für die Bewertung der Behandlung und damit Voraussetzung für die Wahrnehmung der medizinischen Selbstbestimmung und des medizinischen Rechtsschutzes.

5.2.2 Auskunft über Arztbesuche

Ein Bürger verlangte von der Kassenärztlichen Vereinigung Berlin (KVB) eine Aufstellung über seine Arztbesuche in den letzten zehn Jahren. Die KVB war der Auffassung, dass Versicherte ihr gegenüber keinen Auskunftsanspruch hinsichtlich der von ihren behandelnden Vertragsärzten abgerechneten Leistungen hätten. Ein solcher bestünde nur gegenüber der jeweiligen Krankenkasse sowie gegenüber dem Vertragsarzt selbst.

Die KVB hat zwar zutreffend darauf hingewiesen, dass ein Anspruch auf Auskunft über die in Anspruch genommenen Leistungen und deren Kosten nach § 305 Abs. 1 Sozialgesetzbuch Fünftes Buch (SGB V) nur gegenüber der jeweiligen gesetzlichen Krankenkasse besteht. Der betroffene Bürger kann aber gleichwohl den allgemeinen Auskunftsanspruch nach § 83 Sozialgesetzbuch Zehntes Buch (SGB X) gegenüber der KVB geltend machen und Auskunft über die zu seiner Person gespeicherten Sozialdaten verlangen.

Der Anspruch nach § 83 SGB X besteht neben dem des § 305 SGB V. Die Vorschriften stehen nicht in einem sich ausschließenden Spezialitätsverhältnis, da sie inhaltlich völlig unterschiedliche Ziele verfolgen. § 305 SGB V verfolgt den Zweck, das Kostenbewusstsein der Versicherten zu stärken und die Transparenz des Abrechnungsgeschehens zu erhöhen, da aufgrund des Sachleistungsprinzips der gesetzlichen

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Krankenversicherung der Versicherte nicht automatisch Kenntnis über die abgerechneten Leistungen erhält. In § 83 SGB X wird hingegen – analog zu § 19 Bundesdatenschutzgesetz (BDSG) – der Auskunftsanspruch des Versicherten gegenüber jeder Kassenärztlichen Vereinigung über alle den Versicherten betreffenden dort gespeicherten Sozialdaten geregelt. Er geht weiter als der Anspruch aus § 305 SGB V und dient dem Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen. Diese sollen anhand der Daten die Rechtmäßigkeit der Speicherung und die Richtigkeit der Daten beurteilen können.

Der Petent hatte die Art der Daten, über die Auskunft erteilt werden sollte, näher bezeichnet und damit die Antragsvoraussetzungen nach § 83 Abs. 1 Satz 2 SGB X hinreichend erfüllt. Das Auskunftsrecht erstreckt sich auf alle tatsächlich bei der KVB gespeicherten Sozialdaten gem. § 67 Abs. 1 SGB X. Es begründet selbst keine Speicherpflichten. Die Verarbeitungsbefugnisse für Versichertendaten ergeben sich allein aus § 285 Abs. 2 SGB V. Eine Löschung der bei der KVB vorhandenen Behandlungsdaten hat in der Regel spätestens nach 4 Jahren zu erfolgen (vgl. § 304 Abs. 1 SGB V i. V. m. § 84 Abs. 2 SGB X).

Über die Art und Weise der Auskunftserteilung entscheidet die KVB nach pflichtgemäßem Ermessen. Unter Berücksichtigung der Kriterien der bestmöglichen Zweckerfüllung und der Vermeidung von Behinderungen im übrigen Verwaltungsablauf kann sie etwa zwischen der Erlaubnis von Einsichtsmöglichkeiten, dem Anfertigen von Kopien oder der mündlichen Auskunftserteilung wählen. Legitimes Kriterium können auch die für die Auskunftserteilungsart anfallenden Aufwendungen sein. Eine besondere Aufbereitung der Daten braucht nicht zu erfolgen. Verkürzt oder verschlüsselt gespeicherte Daten sind dem Betroffenen allerdings verständlich zu erläutern.

Soweit die KVB geltend macht, dass das Zusammenführen versichertenbezogener Daten über das in § 305 SGB V geregelte Verfahren hinaus regelmäßig mit einem unverhältnismäßigen Verwaltungsaufwand verbunden sei, und hierbei auf die eingeschränkte Auskunftspflicht nach § 83 Abs. 2 SGB X verweist, ist zu bemerken, dass die Ausnahmeregelung des Absatzes 2 nur dann eingreift, wenn es sich um Sozialdaten handelt, die allein deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen. Die Norm bezieht sich mithin auf sog. archivierte Sozialdaten, deren Kenntnis der speichernden Stelle für die rechtmäßige Aufgabenerfüllung nicht mehr erforderlich ist. Dass es sich bei den von dem Petenten begehrten Informationen gerade um solche Daten handelt, war nicht erkennbar.

Im Ergebnis hat sich die KVB – unter teilweiser Aufrechterhaltung ihrer Rechtsposition – dazu bereit er-

klärt, dem Petenten eine Aufstellung über die noch bei ihr verfügbaren Behandlungsdaten der letzten vier Jahre zukommen zu lassen. Wir haben damit den Auskunftsanspruch aus § 83 SGB X als erfüllt angesehen. Über die davor liegenden Zeiträume konnte zu Recht nur eine Negativauskunft erteilt werden.

Die Kassenärztliche Vereinigung Berlin unterliegt – genau wie jede andere datenschutzrechtlich verantwortliche Stelle – der Auskunftspflicht über die bei ihr gespeicherten personenbezogenen Daten.

5.2.3 Bitte lächeln! – Fotos in der *Arztpraxis*

Eine Bürgerin beschwerte sich darüber, dass sie vor der Behandlung in einer HNO-Gemeinschaftspraxis aufgefordert wurde, sich fotografieren zu lassen. Auf unsere Bitte um Stellungnahme teilten die betreffenden Ärzte mit, dass die Fotos der Patienten nicht zu Behandlungszwecken angefertigt würden, sondern zum Zwecke der eindeutigen Identifizierung und damit zur Bekämpfung des Missbrauchs von Krankenversichertenkarten. Jeder Patient würde über die Einarbeitung eines passbildähnlichen digitalen Fotos in seine elektronische Patientenakte ausreichend informiert.

Das von der HNO-Gemeinschaftspraxis praktizierte Verfahren ist datenschutzrechtlich nicht zulässig:

Das Anfertigen eines *Digitalfotos* von jedem Patienten und die Einarbeitung des Fotos in die Personalien der elektronischen Patientendatei stellen eine Erhebung und Verarbeitung personenbezogener Daten dar. Diese sind nach § 4 Abs. 1 BDSG nur zulässig, soweit dafür eine gesetzliche Erlaubnis besteht oder der Betroffene eingewilligt hat.

Eine spezielle Rechtsvorschrift, die eine solche Datenverarbeitung erlaubt, ist nicht ersichtlich. Der Gesetzgeber hat es bislang vielmehr als ausreichend angesehen, dass sich der Patient über seine Krankenversichertenkarte identifiziert. Erst mit der Erweiterung der Krankenversichertenkarte zur elektronischen Gesundheitskarte wird auch ein Lichtbild des Karteninhabers aufgebracht, um die eindeutige Zuordnung der Karte zum jeweiligen Karteninhaber zu verbessern und damit den Missbrauch zu verhindern (vgl. § 291 a i. V. m. § 291 Abs. 2 Satz 1 SGB V) [77]. Das Anfertigen eines Fotos ist auch nicht zur Durchführung des eigentlichen Behandlungsvertrags erforderlich. Es kann derzeit daher lediglich auf der Basis einer Einwilligung der Patienten rechtmäßig erfolgen.

Eine datenschutzrechtliche *Einwilligung.* ist nach § 4 a Abs. 1 BDSG aber nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die erforderliche Freiwilligkeit wird nur dann sichergestellt, wenn

[77] zur elektronischen Gesundheitskarte JB 2005, 4.5.1

die ärztlichen Leistungen nicht an die Bereitschaft der Patienten, in die Verwendung bestimmter sie betreffender Daten einzuwilligen, gekoppelt wird. Die Verknüpfung vertraglicher Leistungen mit dem Zugriff auf weitere für die konkrete Leistung nicht benötigte Angaben ist grundsätzlich nicht zulässig. Sollte daher ein Patient die Einwilligung nicht erteilen wollen, kann nicht allein aus diesem Grund die weitere Behandlung verweigert werden. Weiterhin sind die Patienten vor der Einwilligung auf den vorgesehen Zweck der Erhebung und Verarbeitung hinzuweisen. Die Einwilligung bedarf der Schriftform.

Wir haben die Gemeinschaftspraxis daher aufgefordert, die bisherige Verfahrensweise umzustellen und von den Patienten künftig eine schriftliche Einwilligungserklärung zu verlangen. Ferner waren die bisher unzulässig gespeicherten Patientenfotos zu löschen. Die daraufhin vorgelegte Einwilligungserklärung wurde von uns akzeptiert.

Das Anfertigen von Fotos der Patienten bei dem Besuch einer Arztpraxis ist ohne eine entsprechende Einwilligung datenschutzrechtlich nicht zulässig.

5.2.4 Aufzeichnung von Telefongesprächen beim Ärztlichen Bereitschaftsdienst

Eine Petentin wandte sich an uns mit der Frage, ob es datenschutzrechtlich zulässig sei, dass die Kassenärztliche Vereinigung Berlin Telefongespräche zwischen den Beratungsärzten in der Leitstelle ihres Ärztlichen Bereitschaftsdienstes und den hilfesuchenden Anrufern automatisiert aufzeichnet.

Die Funktion der Telefonzentrale für den Ärztlichen Bereitschaftsdienst besteht darin, den Anrufern den Besuch eines Bereitschaftsarztes zu vermitteln. In der Leitstelle sind durchschnittlich 5 bis 7 (nichtärztliche) Mitarbeiter der Kassenärztlichen Vereinigung Berlin (KVB) tätig. Zudem ist aus Gründen der Qualitätssicherung ein Arzt anwesend. Der Anrufer, der die Telefonnummer des Ärztlichen Bereitschaftsdienstes wählte, hörte bisher folgende Ansage:

„Guten Tag, Sie sind mit dem Ärztlichen Bereitschaftsdienst der Kassenärztlichen Vereinigung Berlin verbunden. Wir weisen aus datenschutzrechtlichen Gründen darauf hin, dass alle Gespräche aufgezeichnet werden.“

Im Anschluss daran wird der Anrufer zum nächsten freien Mitarbeiter weitergeleitet. Dieser nimmt die erforderlichen Daten des Patienten auf (Adressangaben, Namen, Vornamen, Alter, Telefonnummer, Krankenkasse und das jeweilige Beschwerdebild). Anrufer werden nur dann mit dem anwesenden Beratungsarzt verbunden, wenn sich aus dem Gespräch ein besonderes Erfordernis hierfür ergibt, z. B. weil ein unklares Beschwerdebild vorliegt, längere Wartezeiten bis zum

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Eintreffen des Bereitschaftsarztes zu erwarten sind oder ein sofortiger Einsatz des Rettungsdienstes der Feuerwehr angezeigt ist.

Die KVB ist der Auffassung, dass die automatisierte Aufzeichnung der Telefongespräche im Interesse der anrufenden Patienten liege und zwingend notwendig sei. Dies gelte insbesondere im Hinblick auf besondere Notsituationen oder akustische Übermittlungsfehler, etwa bei Namens- und Anschriftenverwechselungen, die sich nur durch das Abspielen der Aufzeichnung aufklären lassen. Die Aufzeichnung diene auch der verlässlichen und nach-prüfbaren Dokumentation zur Sicherung der Beweislage, da die Krankenkassen bei unterbliebenem oder zu spät erfolgtem Notfalleinsatz möglicherweise haften müssten. Die gespeicherten Gespräche sind für die Mitarbeiter der Telefonzentrale 24 Stunden lang abrufbar. Danach werden sie archiviert und nach vier Jahren gelöscht.

Wir haben die Aufzeichnung der Gespräche zwischen den nichtärztlichen Mitarbeitern und den hilfesuchenden Anrufern als datenschutzrechtlich zulässig erachtet. Die damit verbundene Erhebung und Speicherung personenbezogener Daten ist für die Erreichung der von der KVB verfolgten Zwecke erforderlich. Entgegenstehende schutzwürdige Belange der Betroffenen sind nicht ersichtlich.

Notwendig ist allerdings eine angemessene Information der betroffenen Anrufer vor der Aufzeichnung, die auch den Zweck der Speicherung umfasst. Der bisherige Hinweis auf datenschutzrechtliche Gründe ging insoweit fehlt. Wir haben der KVB daher vorgeschlagen, die Eingangsansage wie folgt zu fassen:

„Guten Tag, Sie sind mit dem ärztlichen Bereitschaftsdienst der Kassenärztlichen Vereinigung Berlin verbunden. Um Übermittlungsfehler zu vermeiden, werden zu Ihrer Sicherheit alle Gespräche aufgezeichnet.“

Die KVB hat diesen Vorschlag mittlerweile umgesetzt.

Was die Aufzeichnung der Telefongespräche mit dem Beratungsarzt in der Leitstelle angeht, so kann sich die KVB nicht auf die oben genannten Zwecke berufen. Die Aufzeichnung eines Arzt-Patienten-Gesprächs geht zudem über die in den Berufsordnungen der Ärzte vorgesehenen Dokumentationspflichten hinaus und wird auch nicht von den für die Kassenärztlichen Vereinigungen einschlägigen Verarbeitungsbefugnissen des Sozialgesetzbuchs Fünftes Buch (SGB V) erfasst. Nicht zuletzt ist in diesem Zusammenhang die *ärztliche Schweigepflicht* zu berücksichtigen, der auch die im Rahmen einer telefonischen Beratung dem Arzt anvertrauten Informationen unterliegen.

Vor diesem Hintergrund haben wir gefordert, dass die Entscheidung, ob aufgezeichnet wird oder nicht, dem Anrufer selbst überlassen bleibt. Dem wurde von der KVB dadurch Rechnung getragen, dass nunmehr vor der Weiterleitung an den diensthabenden Beratungsarzt der Anrufer einen zweiten Ansagetext folgenden Inhalts hört:

„Bitte haben Sie einen Moment Geduld. Sie werden mit unserem Beratungsarzt verbunden. Sofern Sie mit der Aufzeichnung des Beratungsarztgesprächs nicht einverstanden sind, informieren Sie bitte unseren Beratungsarzt zu Beginn des Gesprächs."

Sollte der Anrufer der Gesprächsaufzeichnung widersprechen, wird diese durch den Beratungsarzt unterbrochen.

Das Recht auf informationelle Selbstbestimmung wird nur gewahrt, wenn der Anrufer eine transparente und wirksame Möglichkeit hat, die Aufzeichnung des Telefongesprächs mit einem Arzt zu verhindern.

5.2.5 Einnahmen sind nicht gleich Ausgaben – Beitragsberechnung für freiwillig versicherte Mitglieder der AOK Berlin

Uns liegen mehrere Beschwerden freiwillig Versicherter bei der AOK Berlin vor, die sich gegen einen neu gestalteten Fragebogen für die Einkommensprüfung wenden. Während für die Beitragsberechnung bisher lediglich erfragt wurde, ob Leistungen zum Lebensunterhalt von Dritten bezogen werden, sollten nunmehr auch weitreichende Angaben zu den monatlichen Ausgaben für Wohnen, Lebensmittel, Kleidung, Fahrtkosten usw. sowie zu den erhaltenen Sachleistungen gemacht werden. Der Fragebogen wird ausschließlich für die Einkommensprüfung der Mitglieder eingesetzt, deren Beiträge aus dem gesetzlich festgelegten Mindesteinkommen für die Beitragsbemessung berechnet werden.

Als Rahmenbedingung schreibt § 240 Abs. 1 Satz 2 SGB V für die Beitragsbemessung zur freiwilligen Krankenversicherung vor, dass die Beitragsbelastung die gesamte wirtschaftliche Leistungsfähigkeit des freiwilligen Mitglieds berücksichtigen muss. Der Beitragsberechnung dürfen somit nicht pauschal bestimmte Einnahmen zum Lebensunterhalt unterstellt werden, ohne dass die wirtschaftliche Leistungsfähigkeit konkret und individuell geprüft wird. Eine Prüfung der Verhältnisse im Einzelfall hinsichtlich der tatsächlich erzielten Einnahmen ist daher rechtlich erforderlich und die Krankenkasse gemäß § 284 Abs. 1 Nr. 3 SGB V auch berechtigt, die für Beitragsberechnung insoweit erforderlichen Daten zu erheben. Die gesetzliche Regelung geht aber davon aus, dass die Beiträge freiwillig versicherter Mitglieder lediglich nach den aktuellen Einnahmen bemessen werden. Daten zu den monatlichen Ausgaben zählen daher ge-

rade nicht mehr zu den für die Beitragsbemessung unmittelbar erforderlichen Angaben. Eine pauschale Abfrage derselben mittels Fragebogen ist unzulässig.

Die AOK Berlin hat uns gegenüber deutlich gemacht, dass sie auf zusätzliche Angaben angewiesen ist, um den Anforderungen der Prüfdienste des Bundes und der Länder nachzukommen und die Beitragseinstufung plausibel zu machen. In bestimmten Fällen bestehe Anlass zu der Vermutung, dass der Versicherte seiner Pflicht, wahrheitsgemäße und vollständige Angaben bezüglich seines tatsächlich erzielten monatlichen Einkommens zu machen, nicht nachkommt. Im Interesse der Beitragsgerechtigkeit bestehe dann die Notwendigkeit, die Auskünfte der Versicherten genauer zu hinterfragen.

Um den Interessen der betroffenen Versicherten als auch denen der Krankenkasse angemessen Rechnung zu tragen, wurde folgendes Verfahren vereinbart:

In dem künftig zu verwendenden Fragebogen für die Einkommensprüfung derjenigen Mitglieder, deren Beiträge aus dem Mindesteinkommen für die freiwillige Versicherung festgesetzt wurden, wird wieder auf die Angaben zu den monatlichen Ausgaben verzichtet. Zusätzlich wird allerdings ein Feld für die Bestätigung von Unterhaltsleistungen durch Dritte (z. B. Ehegatte, Lebenspartner, Eltern, Freunde, Bekannte etc.) in den Fragebogen aufgenommen. Die Unterhaltsbestätigung durch Unterschrift des Unterhaltsleistenden wird ausdrücklich als freiwillig deklariert. Dem Versicherten bleibt es danach überlassen, erhaltene Unterhaltsleistungen auch auf andere geeignete Weise (z. B. durch Vorlage eines Unterhaltstitels oder einer formlosen Unterhaltsbestätigung) zu belegen. Lediglich in besonders gelagerten Einzelfällen bei Vorliegen konkreter Anhaltspunkte für Falschangaben – etwa wenn der Versicherte keinerlei Einnahmen zum Lebensunterhalt deklariert – behält sich die AOK die Durchführung einer gesonderten Plausibiltätsprüfung vor. Diese kann eine weitere Datenerhebung rechtfertigen.

Eine generelle Erhebung von Daten zu den monatlichen Ausgaben in Form der Abfrage mittels Fragebogen ist für die Beitragsbemessung bei freiwillig versicherten Mitgliedern in der gesetzlichen Krankenversicherung nicht erforderlich und damit unzulässig.

5.2.6 Mammographie-Screening Berlin - datenschutzgerechter Start

Von ihrer Gynäkologin erhielt eine Berlinerin, die über 50 Jahre alt ist, einen Flyer mit dem Hinweis auf das Mammographie-Screening. Die Frau rief unter der angegebenen Telefonnummer an, wurde nach ihrem Namen und ihrem Geburtsdatum gefragt. Im Rahmen des Gesprächs erfuhr sie, dass ihre Daten dort schon gespeichert sind und dass diese dem Mel-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

deregister entstammen.

Die Fragen der Petentin nach der Zulässigkeit der Datenerfassung konnten schnell beantwortet werden. Die Mitarbeiterin der Zentralen Stelle Mammographie-Screening in Berlin erläuterte, dass diese Einrichtung eine öffentliche Stelle des Landes Berlin ist und auf der Grundlage eines Berliner Landesgesetzes arbeitet, das im Mai 2006 vom Abgeordnetenhaus verabschiedet wurde. Danach darf diese Zentrale Stelle, um die Frauen zum Mammographie-Screening einzuladen, Meldedaten aller Frauen zwischen 50 und 69 Jahren verarbeiten.

In unseren Jahresberichten 2004 und 2005[78] machten wir auf eine Reihe von rechtlichen Problemen aufmerksam, die nunmehr durch dieses Gesetz (Mammographie-Screening-Meldedatenverwendungsgesetz) sowie die kurz bevorstehende Änderung des Staatsvertrages über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Sachsen und Thüringen[79] ausgeräumt sind. Die erste von vier Berliner Untersuchungseinrichtungen (Screening-Einheiten) hat parallel zur Zentralen Stelle für das Einladungswesen im Juli ihre Arbeit aufgenommen. Drei weitere Screening-Einrichtungen werden im Januar bzw. im April 2007 hinzukommen. Damit können pro Woche rund 4.000 Frauen eingeladen und durch die Einrichtungen untersucht werden, so sie dies wünschen. Nach der Einladung und ggf. der Erinnerung durch die Zentrale Stelle werden dort die Meldedaten gelöscht. Lediglich zwei Kennnummern werden gespeichert, mit denen zum einen die Qualität der Untersuchung und zum anderen der Mindestabstand von zwei Jahren zwischen den Einladungen gesichert wird.

Drei weitere Screening-Einrichtungen **sind** im Januar bzw. April 2007 hinzugekommen.

Vor Versand der ersten Einladungen prüften wir insbesondere anhand der Unterlagen das verwendete Softwareprogramm. Dabei zeigte sich, dass dieses Programm eine Löschung der identifizierenden Daten, wie Namen, Anschrift, Geburtsdatum nicht vorsah. Wir verlangten eine umgehende Nachbesserung, die im III. Quartal 2006 umgesetzt wurde. Neben der Einladung durch die Zentrale Stelle besteht aber parallel die Möglichkeit, dass sich Frauen durch einen Anruf - wie eingangs geschildert - dort selbst anmelden und einen Untersuchungs-Wunschtermin vereinbaren.

Bis zum Jahresende wurden rund 15.900 Frauen in datenschutzgerechter Weise durch die Zentrale Stelle eingeladen und nahmen zu einem großen Teil das Angebot einer Vorsorgeuntersuchung durch Mammographie an.

[78] JB 2004, 4.4.2; JB 2005, 4.5.1

[79] GVBl. 2006, 1170

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

5.2.7 *Qualitätssicherung.* im Gesundheitswesen - unsere Vorschläge werden aufgegriffen

Im Jahresbericht 2005 legten wir unsere Forderungen zur Sicherung der ärztlichen Schweigepflicht auch bei der Qualitätssicherung im Gesundheitswesen dar. Eine Kernforderung war es, eine gesetzliche Befugnis im Sozialgesetzbuch V zu schaffen, die auf der einen Seite die ärztliche Schweigepflicht und die Rechte der Patienten sichert, auf der anderen Seite aber erlaubt, Gesundheitsdaten für die Qualitätssicherung zu verarbeiten.

Der an vielen Stellen kontrovers diskutierte Entwurf der Bundesregierung zu einer weiteren *Gesundheitsreform* griff unsere Vorschläge weitgehend auf. Damit soll ein für alle Bereiche der Gesundheitsvorsorge (gleich ob Krankenhaus, Arzt- und Zahnarztpraxen, Rehabilitationseinrichtungen) gleiches datenschutzrechtliches Dach für die Qualitätssicherung geschaffen werden. Die Unterschiede im Detail der einzelnen Versorgungssektoren sollen dann in Richtlinien des Gemeinsamen Bundesausschusses von Ärzten und Krankenkassen ihren Niederschlag finden. Dass diese Teile aus dem Gesetzentwurf der Gesundheitsreform nicht kontrovers diskutiert werden, ist im gewissen Umfang auch der Lohn für unsere seit über 10 Jahren währenden Anstrengungen, die Qualitätssicherung zunächst auf freiwilliger Basis in der Dialyse (*QuaSi-Niere.*) datenschutzgerecht zu etablieren. Bei diesem Projekt der Qualitätssicherung werden die Klarnamen und Anschriften der Patienten wie auch der beteiligten Behandlungseinrichtungen von einem Notar verwaltet, der die medizinischen Daten mit Einwilligung der Betroffenen nur unter Pseudonym an die auswertende Stelle (QuaSi-Niere) weitergibt. Gleichzeitig sichert dieser Notar aber auch die Rechte, insbesondere die der Patienten, wenn sie Auskunft über ihre gespeicherten Gesundheitsdaten erhalten wollen.

Das Quasi-Niere Projekt erfuhr 2006 auch internationale Anerkennung. Es wurde in Madrid anlässlich des III. Europäischen Seminars über beispielhafte Lösungen zur Sicherung des Datenschutzes unter 65 eingereichten Arbeiten mit einem von vier vergebenen Preisen ausgezeichnet.

Wenn der Bundesgesetzgeber nunmehr, um eine flächendeckende Qualitätssicherung durchzusetzen, die Verarbeitung von medizinischen Daten gesetzlich Krankenversicherter verpflichtend regelt, greift er die bisherigen Erfahrungen auf. Die Daten sollen pseudonymisiert durch eine unabhängige Stelle ausgewertet und die Patienten in geeigneter Weise qualifiziert informiert werden. Es soll ausgeschlossen werden, dass Krankenkassen und Kassenärztliche Vereinigungen über die Qualitätssicherungsmaßnahmen zusätzliche medizinische Daten der Patienten erlangen. Eine Zweckänderung für die wissenschaftliche Forschung soll aber möglich werden.

Die Bundesregierung hat unsere Vorschläge für eine datenschutzgerechte Qualitätssicherung, insbesondere durch Maßnahmen der Pseudonymisierung und der strikten Trennung des Zugriffs auf die identifizierenden Daten und die medizinischen Daten, im Gesetzentwurf für die Gesundheitsreform aufgegriffen.

5.3 Personaldatenschutz

5.3.1 Umgang mit Disziplinarvorgängen in einer Behörde

Ein Beamter hatte sich für den Dienstposten einer höheren Besoldungsgruppe beworben. Wegen der möglichen Fehlerhaftigkeit des Auswahlverfahrens im Hinblick auf ein gegen ihn anhängiges Disziplinarverfahren hatte er Klage beim Verwaltungsgericht erhoben. Die Prozessbearbeiterin der Behörde nahm in der Antragserwiderung nicht nur auf das im Verfahren relevante Disziplinarverfahren Bezug, sondern fügte einen Vermerk der Disziplinarsachbearbeiterin und einen Entwurf der beabsichtigten Disziplinarverfügung dem Erwiderungsschriftsatz bei. Eine Zustimmung zur Bekanntgabe dieser Daten hatte der Betroffene nicht abgegeben.

Disziplinarvorgänge betreffen den Beamten und stehen mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang. Damit besitzen sie Personalaktenqualität und unterfallen bezüglich ihres Umganges den Vorschriften der §§ 56 ff. Landesbeamtengesetz (LBG).

Prozessbearbeiter sind die Prozessbevollmächtigten der jeweiligen (öffentlichen) Stelle und damit berechtigt und gehalten, prozessrelevante Unterlagen dem Gericht vorzulegen. Insoweit war die Prozessbearbeiterin nach § 56 Abs. 2 LBG befugt, dem Gericht Auskünfte aus dem Disziplinarvorgang zu erteilen. Dabei war jedoch der Grundsatz der Erforderlichkeit bezüglich des Umfanges der Auskunft wegen der hohen Sensibilität von Personalaktendaten besonders sorgfältig zu prüfen.

In dem zu beurteilenden Fall hatte die Prozessbearbeiterin nun versucht, den Vorwurf des Petenten zu entkräften. Dazu hätte es jedoch nicht zusätzlich der Übersendung des Vermerks der Disziplinarsachbearbeiterin sowie des Entwurfs der beabsichtigten Disziplinarverfügung bedurft. Hier hätte ein Hinweis auf diese Unterlagen an das Gericht genügt. Das Gericht hätte dann selbst darüber entscheiden können, ob diese Schriftstücke noch zusätzlich angefordert werden sollen oder nicht. Da im Übrigen im Verwaltungsgerichtsverfahren der Amtsermittlungsgrundsatz gilt, sollte bei diesem sensiblen Datenmaterial grundsätzlich eine entsprechende Anforderung des Gerichts abgewartet werden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Behörde will künftig entsprechend verfahren.

Die verantwortliche Stelle hat genau zu prüfen, welche Unterlagen aus der *Personalakte*, die aufgrund ihrer besonderen Qualität einer gesteigerten Geheimhaltungspflicht unterliegt, an das Gericht weitergegeben werden können.

5.3.2 Das versehentlich weitergegebene *Attest* des Hausarztes

Eine Beschäftigte des Landes Berlin hatte einen Antrag auf Arbeitszeitverkürzung bei ihrer Dienststelle gestellt. Diese entschied daraufhin, zuvor eine amtsärztliche Untersuchung durchführen zu lassen. Im Rahmen dieser Untersuchung übergab die Beschäftigte der Amtsärztin ein Attest ihres behandelnden Hausarztes zur Kenntnisnahme. Die Amtsärztin sicherte der Beschäftigten zu, dieses Attest nicht an die Personalstelle des Landesverwaltungsamtes weiterzuleiten. Aufgrund eines Versehens geschah dies dennoch. Das Landesverwaltungsamt wiederum übersandte sowohl das ärztliche Gutachten als auch das privatärztliche Attest an die Dienststelle der Beschäftigten, wo es ausgewertet wurde. Die Bitte der Beschäftigten auf Entfernung des versehentlich übermittelten privatärztlichen Attestes lehnte das Landesverwaltungsamt ab. Zur Begründung trug es vor, das Attest sei Grundlage für weitere Personalentscheidungen und damit Gegenstand der Personalakte geworden.

Grundsätzlich hat der Auftraggeber einer amtsärztlichen Untersuchung, hier die Dienststelle der Beschäftigten, ausschließlich das Ergebnis der Untersuchung sowie dessen Folge zur Kenntnisnahme zu erhalten.

Auch konnte im vorliegenden Fall nicht nachvollzogen werden, weshalb sich insbesondere das privatärztliche Attest auf dienstliche Maßnahmen ausgewirkt haben soll. Ein privatärztliches Attest kann sich allenfalls unterstützend und bestätigend auf die im Übrigen grundsätzlich unabhängigen Entscheidungen des Amtsärztlichen Dienstes auswirken. Das Untersuchungsergebnis ermittelt der Amtsarzt eigenständig und souverän. Er kann sich dabei die Einschätzung des behandelnden Arztes zu eigen machen oder auch nicht. Damit hat ausschließlich die Entscheidung des Amtsarztes über die beantragte Arbeitszeitverkürzung Auswirkungen auf dienstliche Maßnahmen, nicht dagegen ein privatärztliches Attest der Betroffenen, insbesondere wenn dies auch noch versehentlich zur Personalakte gelangt ist.

Versehentlich an die Dienststelle übersandte privatärztliche Atteste sind grundsätzlich unverzüglich den Beschäftigten auszuhändigen und darüber hinaus sämtliche diesbezüglichen Vermerke oder Ausführungen aus der *Personalakte* zu entfernen bzw. zu schwärzen.

Das vom Berliner Beauftragten für Datenschutz und Informationsfreiheit „bemängelte Verfahren“ war schlussendlich Gegenstand einer Klage vor dem Arbeitsgericht. Dieser Arbeitsrechtsstreit wurde durch arbeitsgerichtlichen Vergleich mit der Folge beendet, dass das privatärztliche Attest „vertraulich, verschlossen“ in der Personalakte verblieb und Hinweise auf dieses privatärztliche Attest in diversen Schreiben sowohl des Statistischen Landesamtes Berlin als auch des Landesverwaltungsamtes Berlin zu schwärzen waren.

Das Landesverwaltungsamt hat dafür Sorge zu tragen, dass die Beschäftigungsstelle lediglich das Ergebnis der amtsärztlichen Untersuchung zur Kenntnis erhält, nicht jedoch das Gutachten selbst. Dieses ist, falls der Amtsärztliche Dienst nicht nur das Ergebnis der Untersuchung übersendet, in einem verschlossenen Umschlag zur Personalakte des Beschäftigten zu nehmen.

5.3.3 ADONIS – Modellierung und Dokumentation von Geschäftsprozessen

Der behördliche Datenschutzbeauftragte einer Senatsverwaltung wurde pflichtgemäß von seiner Behörde darüber informiert, dass sie beabsichtige, die von der Senatsverwaltung für Inneres beschafften Lizenzen für die Software ADONIS für die Modellierung und Dokumentation von Geschäftsprozessen mitzunutzen. Er wurde ferner darüber unterrichtet, dass bereits 57 Stellen im Land Berlin das Programm nutzen. Das Programm ermögliche es auch, den einzelnen zu analysierenden Arbeitsschritten nicht nur abstrakte Rollen, sondern auch konkrete Personen zuzuordnen. Der behördliche Datenschutzbeauftragte wollte sich aus der Sicht des Datenschutzes ein Bild machen und bat uns um Unterstützung, zumal er erwarten durfte, dass wir bei einem so verbreitet eingesetzten Verfahren zur Verarbeitung von Personaldaten längst nach § 24 Abs. 3 Satz 3 Berliner Datenschutzgesetz (BlnDSG) unterrichtet worden wären.

Dies war aber keineswegs der Fall. Nachdem wir die Senatsverwaltung dreimal angeschrieben und im letzten Schreiben eine Beanstandung wegen fehlender Unterstützung angedroht hatten, erhielten wir drei Monate nach der ersten Anfrage endlich Informationen über ADONIS. Kurz zuvor war ADONIS der landesweiten Nutzung entzogen worden, weil der Abschluss einer Dienstvereinbarung mit dem Hauptpersonalrat nicht vorlag. In der Beteiligungsvorlage an den Hauptpersonalrat war ein Passus enthalten, der den Umgang mit personenbezogenen Daten betraf. Er versprach eine *Pseudonymisierung* der Daten, die jedoch mit außerhalb des Systems vorliegenden Zuordnungslisten wieder aufgehoben werden konnte. Damit konnte der Personenbezug wieder hergestellt werden und der Hauptpersonalrat befürchtete zu Recht, dass personenbezogene Leistungs- und Verhaltenskontrollen damit nicht ausgeschlossen werden können.

In unserer Stellungnahme monierten wir die zweideutige Zusicherung, auf den Personenbezug unter bestimmten Bedingungen zu verzichten, ihn aber andererseits auch wieder herstellen zu können. Wir machten ebenfalls darauf aufmerksam, dass die bereitgestellten Herstellerinformationen zu ADONIS sehr deutlich machten, dass bei der Verarbeitung der Arbeitsplatzanalysedaten personenbezogen Daten einbezogen werden können.

Erfreulicherweise akzeptierte die Senatsverwaltung für Inneres dann, dass für das angestrebte Ziel der Modellierung und Analyse von Geschäftsprozessen der Personenbezug der zu analysierenden Daten unnötig ist, und änderte den bemängelten Passus der Beteiligungsvorlage. Sie versprach, dass mit einer Person verbundene Identifizierungsdaten nicht erfasst werden und dass Auswertungen, die sich auf weniger als drei Personen beziehen lassen, unzulässig sind. Damit waren unsere Bedenken ausgeräumt.

Auch in den Behörden halten Managementsysteme Einzug, die die behördlichen Geschäftsprozesse wie mit ADONIS oder Entscheidungsprozesse (Controlling) analysieren und so zu ihrer Optimierung beitragen können. Solche Verfahren benötigen in der Regel keine personenbezogenen Daten, sondern kommen mit anonymen oder pseudonymen Einzelfalldaten aus. Leider bedarf es immer wieder der Überzeugungsarbeit, um die unter diesen Umständen unzulässige, weil nicht erforderliche Einbeziehung personenbezogener Daten zu unterbinden.

5.3.4 Unverschlüsselter Datenfluss bei einer Arbeitsvermittlung

Ein Arbeitsvermittlungsunternehmen nahm Bewerbungsvorgänge von Arbeitsuchenden als Auftragnehmer entgegen, um sie dann an die aus seiner Sicht geeigneten potenziellen Arbeitgeber zu übersenden. Die Übermittlung der Bewerberdaten erfolgte dabei auf elektronischem Weg und unverschlüsselt. Als Begründung für diese Vorgehensweise legte der Geschäftsführer des Unternehmens dar, eine Verschlüsselung sei mit unverhältnismäßigem technischem und finanziellem Aufwand für sein Unternehmen verbunden und würde sich zudem nachteilig auf die Bewerbungen auswirken, da die meisten Arbeitgeber ebenfalls keine Schlüssel verwenden würden. Verschlüsselte E-Mails würden außerdem häufig von SPAM-Filtern ausgesondert. Im Übrigen würde man die Arbeitsuchenden im Rahmen einer vorformulierten Einwilligungserklärung auf die Risiken der unverschlüsselten Übermittlung ihrer Bewerberdaten hinweisen, sodass die Betroffenen selbst entscheiden könnten, ob sie dieses Verfahren wählen wollen oder nicht.

Bei *Bewerberdaten* handelt es sich um besonders sensitive Daten, deren unsachgemäße Verarbeitung einen schweren Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt. Es ist im Einzelfall weder dem Auftraggeber noch dem Arbeitsvermittler möglich, die konkrete Zahl der Personen zu begrenzen, welche Kenntnis von den Daten der Bewerber erlangen. Gemäß Nr. 4 der Anlage zu § 9 Satz 1 BDSG hat die verantwortliche Stelle zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen,

kopiert, verändert oder entfernt werden können.

Von dieser Gewährleistung kann sich die verantwortliche Stelle nicht befreien, indem sie von den Betroffenen die Unterzeichnung einer Einwilligung verlangt, denn die Umsetzung von § 9 BDSG ist kein Recht des Betroffenen, sondern eine Pflicht des Verarbeiters. Eine Einwilligung nach § 4 a Abs. 1 BDSG in den Verzicht auf technisch-organisatorische Maßnahmen ist auch schon deswegen nicht möglich, weil die Folge bzw. Tragweite eines solchen Verzichts weder für den Betroffenen noch für den Verarbeiter überschaubar wäre. Im Übrigen handelt es sich bei § 9 BDSG um eine zwingende ordnungsrechtliche Vorschrift, die nicht durch eine materiell-rechtliche Regelung (§ 4 a BDSG) aufgehoben werden kann.

Die *Verschlüsselung* ist auch nicht mit einem unverhältnismäßigen technischen und wirtschaftlichen Aufwand verbunden. Durch einfache Korrekturen an der Einstellung der SPAM-Filter ist es leicht möglich, verschlüsselten E-Mails eine positivere Bewertung durch die Filterprogramme zu verschaffen. Es ist davon auszugehen, dass Arbeitgeber, die auf elektronischem Weg erreichbar sind, in der Regel mit Einstellungen ihrer SPAM-Filter arbeiten, die ihnen eine tatsächliche Erreichbarkeit auch mittels verschlüsselter E-Mails erlauben. Selbst wenn es zu einer Aussortierung der E-Mail kommt, bieten moderne Systeme zur SPAM-Filterung die Möglichkeit, die E-Mail in einem zweiten Versuch zuzustellen.

Nach Aussage der PGP Corporation wird ihre Software dabei weltweit von über 30.000 Unternehmen und öffentlichen Verwaltungen eingesetzt. Der Aufwand für das Verschlüsseln einer E-Mail ist gegenüber dem unverschlüsselten Versand zwar geringfügig erhöht, der Zeitaufwand lässt sich aber nach kurzer Einarbeitungszeit auf 10 bis 15 Sekunden pro Mail senken, zuzüglich des einmaligen Aufwandes für das Suchen und Importieren des Schlüssels. Damit steht der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck.

Arbeitsvermittlungsunternehmen sind verpflichtet, durch technische und organisatorische Maßnahmen den größtmöglichen Schutz von sensitiven Bewerberdaten zu garantieren. Die Verschlüsselung der Daten vor ihrer elektronischen Übermittlung ist damit alternativlos für den Schutz der Betroffenen.

5.3.5 Datenschutz als Beitrag zum Betriebsfrieden

Eine anonyme Anzeige bei der Berliner Staatsanwaltschaft wies auf einen vermeintlich schweren Datenschutzverstoß bei der GASAG hin. Danach hatten alle Mitarbeiter einer Abteilung Zugang zu einer Excel-Gehaltsdatei für diese Abteilung, die von einem bestimmten Mitarbeiter geführt wurde. Die Staatsanwaltschaft schaltete daraufhin uns ein.

Wie würden Sie reagieren, wenn Sie erfahren würden, dass Ihr Kollege bei gleicher Tätigkeit mehr verdient als Sie? Die Gefahr einer Störung des Betriebsfriedens lag hier nahe, sodass wir schnell reagierten.

Die Datenschutzbeauftragte der GASAG führte auf unsere Anfrage hin eine Kontrolle der Datenverarbeitung in der betreffenden Abteilung durch. Sie kam zu dem Ergebnis, dass der zuständige Sachbearbeiter bei der Reorganisation der persönlichen Dateiablage die Gehaltsdatei versehentlich in einen ungeschützten Bereich kopiert hatte, sodass alle Mitarbeiter der Abteilung die Datei hätten lesen können. Dem Sachbearbeiter war aus den internen Schulungen jedoch bekannt, dass solche Daten dem Datenschutz unterliegen und vor unbefugtem Zugriff zu schützen waren. Ansonsten ergaben sich aus der Kontrolle keine Beanstandungen. Der Vorfall wurde als Einzelfall aufgrund unbeabsichtigten Fehlverhaltens eingestuft. Wir baten um den internen Prüfbericht.

Diesen erhielten wir mit der Beantwortung einiger zusätzlicher Fragen. Danach speicherte der Sachbearbeiter die Datei auf seinem persönlichen Laufwerk, weil auf dem Abteilungslaufwerk kein Verzeichnis eingerichtet war, dass nur ihm und der Abteilungsleitung zugänglich gewesen wäre. Dies war natürlich ein Mangel, der nicht dem Sachbearbeiter zuzurechnen war. Nach Satz 1 der Anlage zu § 9 Satz 1 BDSG ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Mangel der Dateiorganisation führte daher zusammen mit einem Versehen zum Mangel der Zugriffskontrolle nach Nr. 3 der Anlage zu § 9 Satz 1 BDSG. Solche Dateien dürfen nicht Gegenstand persönlicher Dateireorganisationen werden, sondern gehören in die Obhut qualifizierter Systemverwalter.

Auf unseren Vorhalt hin wurde ein Verzeichnis auf dem Laufwerk der Organisationseinheit eingerichtet, auf das nur die zuständigen Mitarbeiterinnen und Mitarbeiter Zugriffsrechte besitzen. Der Mangel wurde somit behoben.

Häufig ist festzustellen, dass versehentliches Fehlverhalten einzelner Personen auch auf organisatorische oder technische Mängel zurückzuführen ist, die nicht von ihnen zu vertreten sind.

5.4 Wohnen und Umwelt

5.4.1 Abrufe aus dem Korruptionsregister

Die Senatsverwaltung für Stadtentwicklung unterrichtete uns pflichtgemäß nach § 24 Abs. 3 Satz 3 BlnDSG über die beabsichtigte Umsetzung des Korruptionsregistergesetzes durch ein automatisiertes Abrufverfahren. Dieses Korruptionsregister soll den Aufträge

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

vergebenden Stellen des Landes ermöglichen festzustellen, ob bestimmte Firmen im Zusammenhang mit Korruptionsvorfällen bereits eingetragen worden sind, um dies bei der Auftragsvergabe berücksichtigen zu können.

Mit der Verabschiedung des Gesetzes zur Errichtung und Führung eines Registers über korruptionsanfällige Unternehmen in Berlin[80] hat der Gesetzgeber eine *Transparenz* erhöhende Regelung für das Vergabeverfahren erlassen. Diese Regelung ist grundsätzlich zu begrüßen, auch wenn im Gesetzgebungsverfahren nur ein Teil unserer Empfehlungen berücksichtigt wurde.

Ein automatisiertes Verfahren zum Abruf personenbezogener Daten darf nur eingerichtet werden, wenn dies ein Gesetz ausdrücklich zulässt (§ 15 BlnDSG). Mit § 2 Abs. 2 Korruptionsregistergesetz wurde diese Voraussetzung geschaffen. Eine weitere Voraussetzung ist die Schaffung einer Rechtsverordnung, in der Einzelheiten bei der Einrichtung eines solchen *Abrufverfahrens* zu regeln sind. Dazu gehören neben der Festlegung von Datenempfängern, den Datenarten und Zwecken des Abrufes auch technische und organisatorische Maßnahmen zur Datensicherung und zur Kontrolle der Abrufe.

Zur Diskussion stand auch, welche Daten in dem Verfahren überhaupt abgerufen werden dürfen. Dem Wortlaut des Gesetzes würde es entsprechen, wenn nur mitgeteilt würde, ob eine Eintragung vorliegt oder nicht. Wir haben uns jedoch davon überzeugen lassen, dass diese Angabe nicht ausreicht. Eine Eintragung im Korruptionsregister bedeutet nämlich nicht den automatischen Ausschluss aus dem Vergabeverfahren, sondern erlaubt den anfragenden Vergabestellen abzuwägen, ob nicht dennoch eine Auftragsvergabe sinnvoll sein kann. Für diese Abwägung werden mehr Angaben gebraucht als nur ein „Ja“ oder „Nein“.

Als technische Maßnahme zur Kontrolle der Abrufe sieht das Sicherheitskonzept unserem Vorschlag entsprechend die *Protokollierung* aller Abrufe vor, also auch der Abrufe, die zu einer Fehlanzeige führen, weil das angefragte Unternehmen keinen Eintrag im Korruptionsregister hat. Wegen der hohen Sensitivität der Daten ist dies sachgerecht, wenn man missbräuchliche Ausforschungen im Korruptionsregister unterbinden will. Allerdings sollen nach dem Konzept Protokolleinträge zu Eintragungen, die sich als falsch erwiesen haben, unverzüglich gelöscht werden. Diese Maßnahme haben wir in Zweifel gezogen, weil gerade Abrufe unzutreffender Informationen nachvollziehbar bleiben sollten.

Die Senatsverwaltung hat unseren Empfehlungen

Die Darstellung des Berliner Beauftragten für Daten-

[80] v. 19. April 2006, GVBl., 358

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

nicht widersprochen, sodass wir von einer entsprechenden Modifikation des Konzepts ausgehen.

Berliner Behörden, die Aufträge vergeben, können künftig in datenschutzgerechter Weise Daten aus dem Korruptionsregister abrufen.

5.4.2 Förderdatenbank zur EU-Förderung von Wohnumfeld-Maßnahmen (WUM-Datenbank)

Die Senatsverwaltung für Stadtentwicklung unterrichtete uns ebenfalls über geplante Änderungen eines IT-Verfahrens mit dem launigen Namen WUM zur Kontrolle der EU-Fördermaßnahmen zur Verbesserung des Wohnumfeldes in bestimmten Gebieten Berlins. Da auch Einzelpersonen Empfänger solcher Fördermittel sein können, ist die Datenbank personenbezogen und damit datenschutzrelevant. Die bisher zentral bei der Senatsverwaltung geführte Datenbank dient vor allem der Kontrolle des Mittelabflusses in den Projekten. Da diese aber zunehmend dezentral von den Bezirken gesteuert werden, sollen auch die Bezirke Zugang zur Datenbank erhalten.

Die Bezirke sollen in Zukunft die Pflege der eigenen Projektdaten selbst durchführen. Jeder Bezirk erhält den Zugriff auf sein eigenes Datensegment und ist daher selbst Daten verarbeitende Stelle nach § 4 Abs. 3 Nr. 1 BlnDSG, während die Senatsverwaltung als Auftragnehmerin der Bezirke nach § 3 Abs. 1 BlnDSG die Datenbank betreibt. Da die Senatsverwaltung aber auch eigene Projekte verwaltet, ist sie für ihr Segment selbst Daten verarbeitende Stelle. Weil die Senatsverwaltung außerdem für ganz Berlin die Mittelabflüsse für die EU zu überwachen hat, benötigt sie den lesenden Zugriff auf alle Daten und soll diesen im Rahmen eines automatisierten *Abrufverfahrens* erhalten.

Das Verfahren beruht auf europäischem Recht. Allerdings gibt es keine Rechtsgrundlage für die Errichtung des Abrufverfahrens, die nach § 15 BlnDSG erforderlich wäre. Es stellte sich also die Frage, ob das automatisierte Abrufverfahren auf eine explizite und informierte Einwilligung gestützt werden kann, obwohl § 15 BlnDSG eine solche Option nicht vorsieht.

Unsere rechtliche Prüfung zu der bisher nie aufgeworfenen Frage kam zu dem Ergebnis, dass das automatisierte Abrufverfahren nach Berliner Landesrecht nicht auf eine Einwilligung gestützt werden kann, wenn die Voraussetzungen des § 15 BlnDSG nicht vorliegen.

Allerdings liegt hier eine Sondersituation vor, weil die Daten aufgrund von EU-Recht erhoben werden. Die in der „Aufklärung über die Verarbeitung antragsgebun-

schutz und Informationsfreiheit ist zutreffend. Die von ihm gegenüber der zuständigen Senatsverwaltung für Stadtentwicklung ausgesprochenen Empfehlungen werden in dem modifizierten IT-Sicherheitskonzept berücksichtigt, einschließlich der Protokollierung aller Abrufe.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

dener Daten einschließlich der Verarbeitung personenbezogener Daten“ genannten Rechtsgrundlagen sind zwar überholt, da sie durch neue EU-Verordnungen ersetzt wurden, allerdings enthalten diese jedoch keine Regelungen über die Verarbeitung personenbezogener Daten. Insoweit ist die Vorschrift des § 6 Abs. 2 BlnDSG auf diesen Fall entsprechend anzuwenden. Denn wenn schon bei der Anwendung von Bundesrecht, das keine Verarbeitungsregeln enthält, die §§ 13–15 BDSG heranzuziehen sind, ist das bei der Anwendung entsprechenden EU-Rechts erst recht sachgerecht.

Das ändert allerdings nichts daran, dass auch in einem solchen Fall der im Vergleich zum § 10 BDSG strengere § 15 BlnDSG (Erfordernis einer gesetzlichen Grundlage) anzuwenden ist.

Es sind deshalb zwei Wege erkennbar, wie der *Online-Zugriff* der Senatsverwaltung auf die WUM-Datenbank ermöglicht werden kann:

Es wird ein pseudonymisierter Teilbereich der Datenbank gebildet, auf den die Senatsverwaltung zur Kontrolle des Mittelabflusses zugreifen kann. Stellen sich im Einzelfall Unregelmäßigkeiten heraus, muss die Senatsverwaltung ohnehin den (papiergestützten) Fördervorgang insgesamt beim Bezirk anfordern. Dies genügt auch den Anforderungen der EU-Verordnungen, die den Mitgliedstaaten die Art und Weise der Kontrolle freistellen. Die Mitgliedstaaten müssen nur sicherstellen, dass die Kontrollmechanismen effektiv sind. Im Einzelfall können sowohl die (nationale) Prüfbehörde (in Deutschland das zuständige Bundesfinanzministerium) als auch die Europäische Kommission selbst Einsicht in die Förderakten verlangen.

Das erfordert aber keinen Online-Zugriff der Senatsverwaltung für Stadtentwicklung auf die Förderdaten mit direktem Personenbezug. Zwar vertreten wir die Auffassung, dass auch pseudonymisierte Daten personenbezogen sind, würden aber einen Online-Zugriff auf solche Daten auch ohne gesetzliche Grundlage nach § 15 BlnDSG mit informierter Einwilligung zulassen.

Falls der Online-Zugriff auf direkt personenbezogene Daten durch die Senatsverwaltung entgegen unserer Annahme doch unerlässlich (nicht nur zweckmäßig und bequem für die Verwaltung) sein sollte, sind ein Gesetz und eine Rechtsverordnung nach § 15 BlnDSG zu erlassen.

Auf diese Empfehlungen haben wir bisher nur eine Eingangsbestätigung und die Zusicherung erhalten, dass wir über die Umsetzung der Vorschläge unterrichtet werden.

Ein Online-Zugriff auf Datenbestände einer Berliner Behörde, für den eine gesetzliche Grundlage fehlt, kann auf die Einwilligung der Betroffenen nur dann

Die zuständige Senatsverwaltung für Stadtentwicklung hatte beabsichtigt, bei einer Umsetzung des Vorhabens, den Bezirken unmittelbaren Zugriff auf die WUM-Datenbank einzuräumen, personenbezogene Daten nur noch in pseudonymisierter Form in die Datenbank aufzunehmen. Aufgrund fehlender personeller Ressourcen konnte das Vorhaben in 2006 jedoch nicht mehr umgesetzt werden. Da die Datenbank für die am 01.01.2007 begonnene neue EU-Förderperiode nicht mehr zum Einsatz kommt, ist mittlerweile nicht mehr davon auszugehen, dass das Vorhaben noch umgesetzt wird.

Derzeit befindet sich ein neues Datenbanksystem für die EU-Förderperiode 2007 – 2013 im Aufbau.

Durch Änderungen im Förderverfahren ist davon auszugehen, dass in der Datenbank keine personenbezogenen Daten mehr enthalten sein werden, da kleinteilige Fördervorhaben künftig gebündelt über die Träger des Quartiersmanagement-Verfahrens abgerechnet werden.

Unabhängig hiervon hat sich die Rechtsgrundlage geändert. Die Durchführungsbestimmungen für die Strukturfondsförderung sind nunmehr in der Verordnung (EG) Nr. 1083/2006 geregelt. Die Senatsverwaltung für Wirtschaft, Technologie und Frauen als Verwaltungsbehörde für EU-Strukturfonds geht davon aus, dass mit der Verordnung eine Rechtsgrundlage für einen automatisierten Abruf personenbezogener Förderdaten gegeben wäre Sie hat daher beim Berliner Beauftragten für Datenschutz und Informationsfreiheit im März 2007 eine entsprechende Anfrage gestellt

gestützt werden, wenn er sich auf pseudonymisierte Daten beschränkt.

5.4.3 Die elektronische *Heizkostenberechnung*

Da es kaum noch Lebensbereiche gibt, in die die Elektronik nicht Einzug gehalten hat, wurden wir nun auch mit der elektronischen Verbrauchsmessung zur Berechnung der Heizkosten konfrontiert.

Die Mieter eines Wohnkomplexes, der im Eigentum einer landeseigenen Wohnungsbaugesellschaft stand, informierten uns darüber, dass in den Wohnungen Heizkostenverteiler und Wasserzähler eingebaut wurden, die sechsmal pro Tag im 433-MHz-Band Messergebnisse per Funkübertragung an eine zentrale Empfangsstelle außerhalb der Wohnungen übermitteln. Das Einverständnis der Mieter wurde nicht eingeholt, sondern lediglich eine Informationsbroschüre der Installationsfirma über ihr Produkt per Briefeinwurf verteilt und der Austausch der Heizkostenmessgeräte durch die Auftragsfirma angekündigt.

Die Mieter beschwerten sich darüber, dass ihr Einverständnis dazu nicht eingeholt wurde, und äußerten die Besorgnis, durch die sechsmalige Ablesung und elektronische Meldung an ein zentrales Erfassungsgerät per Funk könnten ihre Lebensgewohnheiten ausgeforscht werden.

Die landeseigenen Wohnungsbaugesellschaften werden als privatrechtlich organisierte Körperschaften tätig. Sie unterliegen den Datenschutzbestimmungen des Bundesdatenschutzgesetzes. Infolgedessen ist die datenschutzrechtliche Bewertung der elektronischen Heizkostenmessung und Berechnung sowie die automatische Übertragung der Messwerte per Funk an eine zentrale Sammelstation für den ganzen privaten Wohnungsmarkt von grundsätzlicher Bedeutung. Zwar hat der Bundesgesetzgeber im Gegensatz zum Berliner Gesetzgeber (§ 31 a BlnDSG) bisher keine spezielle Regelung zu Fernmess- und Fernsehdiensten getroffen, in der Sache sind dem Bundesrecht aber vergleichbare Anforderungen zu entnehmen.

Wenn Gefährdungen des informationellen Selbstbestimmungsrechts der Mieter durch die elektronische *Fernmessung* ausgeschlossen worden sind und das Fernmesssystem dem Schutz des Einzelnen vor Ausspähung und Kontrolle privater Lebensabläufe und Lebensfunktionen in anderer Weise Rechnung trägt, bestehen keine Bedenken gegen die elektronische Fernmessung der Wärmeverbrauchswerte zur Heizkostenberechnung.

Voraussetzung für die unbedenkliche elektronische *Verbrauchsdatenerfassung* und die drahtlose elektronische Übermittlung der Verbrauchsdaten per Funk an eine zentrale elektronische Erfassungsstelle ist demnach Folgendes:

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Der Zeitpunkt der Fernablesung muss den Mietern bekannt sein. Mit anderen Worten: Es dürfen keine heimlichen Ablesungen durchgeführt werden. Die Mitteilung des Zählerstandes muss transparent sein, d. h., sie muss von den betroffenen Mietern gelesen und überprüft werden können. Die Messgeräte müssen für die Betroffenen zugänglich sein. Die Ablesbarkeit in einem Display genügt hierbei. Das Ab- und Auslesen der Daten durch Unbefugte muss ausgeschlossen sein, was z. B. durch Verschlüsselung sichergestellt werden kann.

Verweigern oder widerrufen die Mieter ihre Einwilligung zur Installation eines elektronischen Ablesesystems, können sie mit den Mehrkosten einer traditionellen Ablesung vor Ort belastet werden. Es steht nicht im Widerspruch zum Willen des Gesetzgebers, dass den Betroffenen im Falle einer Verweigerung oder eines Widerrufs der Einwilligung die unmittelbaren Folgekosten aufgebürdet werden. Allerdings toleriert das Datenschutzrecht es nicht, dass den Betroffenen darüber hinausgehende Nachteile entstehen.

Das Fernmessen des Energie- und Wasserverbrauchs in Wohnungen ist nur zulässig, wenn es für die Mieter nachvollziehbar und auf einem sicheren Übertragungsweg erfolgt. Besteht der Mieter auf einer herkömmlichen Ablesung durch einen Mitarbeiter des Versorgungsunternehmens, dürfen ihm nur die dadurch unmittelbar entstehenden Folgekosten berechnet werden.

Auf Grund einer aktuellen Anfrage im April 2007 durch die Senatsverwaltung für Stadtentwicklung haben alle sechs städtischen Wohnungsbaugesellschaften Berlins bestätigt, dass – in Entsprechung der im Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit aufgeführten Kriterien – die schutzwürdigen Interessen der Mieter bei der elektronischen Verbrauchsdatenerfassung nicht beeinträchtigt würden

5.4.4 Im Kleingarten der Informationslüste

Der Parzellenbesitzer eines Kleingartenvereins stellte eines Tages fest, dass sich an den Informationstafeln seiner Siedlung ein personenbezogener Aushang über das Verhalten von Vereinsmitgliedern, d. h. Parzellenbesitzern, befand. Die Vereinssatzung und Mitgliederbeschlüsse des Vereins sahen vor, dass jedes Vereinsmitglied jährlich sechs Arbeitsstunden für den Verein abzuleisten habe. Wer diese Stunden nicht ableisten konnte oder wollte, konnte stattdessen zum Ende des Kalenderjahres eine Geldersatzleistung erbringen. In dem Aushang, der an allen allgemein und öffentlich zugänglichen Informationstafeln angebracht worden war, wurde bekannt gegeben, bei welchen Mitgliedern - im Hinblick auf diese Pflichten – Differenzen bestanden. Es wurden zwar nur die Parzellennummern benannt, aus ihnen konnte jedoch unschwer das jeweilige Vereinsmitglied erkannt werden, da an jeder Parzelle die Parzellennummer und das Namensschild des Besitzers angebracht sind. Über die Parzellennummer waren ohne Schwierigkeit die säumigen Mitglieder zu identifizieren. Der Petent wies darauf hin, dass jedes Vereinsmitglied wisse, ob es seine Arbeitsstunden erbracht habe oder nicht. Deshalb sei es dem Vorstand des Kleingartenvereins nicht um die sachbezogene Information an die betroffenen Mit-

glieder gegangen. Vielmehr sollten die säumigen Mitglieder mit diesem Aushang an den öffentlichen Pranger gestellt werden.

Von einem anderen Verein wurden wir im Hinblick auf etwaige datenschutzrechtliche Probleme vorsorglich gefragt, ob es erlaubt sei, während einer Mitgliederversammlung Schuldner wegen ihrer rückständigen Mitgliedsbeiträge namentlich zu benennen.

Diese beispielhaften Eingaben aus einer Serie vielfältiger ähnlicher Datenschutzprobleme in Kleingarten- oder Siedlervereinen zeigen, dass so manche im Vereinsleben zu Tage getretene Spannung zwischen den Mitgliedern auch zu datenschutzwidrigen Fehlreaktionen führen kann. In der Annahme, „man kenne sich“ oder „jeder wisse doch ohnehin ...“, übersah der Vorstand die auch für das Vereinsleben geltenden Vorschriften der §§ 4 und 28 BDSG. Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben. Wenn die einzelnen Betroffenen nicht in ihre öffentliche und namentliche Benennung, sei es auf der Mitgliederversammlung oder in dem öffentlichen Aushang, eingewilligt haben, ist die Nennung der Namen oder eines gleichbedeutenden Synonyms (wie hier die Parzellennummer) nicht zulässig, erst recht dann nicht, wenn damit eine Information über die Erfüllung oder Nichterfüllung vereinsrechtlicher Pflichten verbundenen ist.

Wenn keine Einwilligung der betroffenen Vereinsmitglieder vorliegt, dass die Namen in der Vereinsöffentlichkeit oder gar in der darüber hinausgehenden Öffentlichkeit erörtert werden dürfen, ist allein auf § 28 BDSG abzustellen. Maßgeblich ist nach § 28 BDSG, ob die Veröffentlichung der Mitgliederdaten der Zweckbestimmung des Vereins im Sinne der Mitgliedschaftsrechte und -pflichten entspricht.

Die Vereinssatzungen der überprüften Vereine enthielten hierzu keine Regelungen. Der Verein steht als juristische Person zu seinen Mitgliedern in einem zweiseitigen Rechtsverhältnis. Er muss zwischen den allgemeinen Belangen des Vereins und den bilateralen rechtlichen Beziehungen des Vereins zu seinen Mitgliedern unterscheiden. Eine gesetzliche Regelung, säumige Vereinsmitglieder öffentlich bekannt zu geben, und sei es auch nur in der vereinsinternen Öffentlichkeit, gibt es nicht. Sie wäre auch nicht sinnvoll. Denn nicht die einzelnen Mitglieder vermögen die rechtlichen Interessen des Vereins gegenüber seinen Mitgliedern im Einzelnen durchzusetzen, sondern nur der mit der Geschäftsführung betraute Vorstand als Vertreter des Vereins ist dazu imstande. Er kann die Vereinsrechte gegenüber seinen Mitgliedern nur bilateral durchsetzen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die öffentliche Anprangerung ist zur Wahrung der Vereinsinteressen weder geeignet noch angemessen, vielmehr ist sie aufgrund der „Prangerwirkung“ unzulässig. Wir haben daher den Vereinen empfohlen, säumige Mitglieder auf Mitgliederversammlungen nicht namentlich zu benennen, sondern etwaige Forderungen ausschließlich individuell gegenüber dem einzelnen Mitglied durchzusetzen. Erst recht haben wir davon abgeraten, die Daten säumiger Mitglieder auf öffentlich zugänglichen Informationstafeln bekannt zu geben, weil mit dieser Art der Bekanntgabe sogar die vereinsinterne Öffentlichkeit überschritten wird und eine Anprangerung gegenüber der allgemeinen Öffentlichkeit erreicht wird, die über die Vereinsgrenzen hinausgeht. Denn die Kleingärten und Siedlungsgemeinschaften sind in der Regel auch öffentlich zugänglich.

Der Anprangerung einzelner Vereinsmitglieder auf Mitgliederversammlungen oder auf öffentlichen Stellwänden liegt eine Informationslust zugrunde, die mit den Rechtsvorschriften des § 28 BDSG unvereinbar ist. Sie verstößt gegen geltendes Recht und verletzt die schutzwürdigen Belange der betroffenen Mitglieder, wenn diese nicht ausdrücklich persönlich zugestimmt haben oder die Maßnahme aus einem Gemeinschaftsakt des Vereins (Mitgliederbeschluss oder Regelung in der Satzung) gerechtfertigt werden kann.

6 Wissen und Bildung

6.1 Wissenschaft und Forschung

6.1.1 Der Teufel steckt im Detail – P*seudonymisierung* bei *Arzneimittelstudien*

Über Jahrzehnte war es üblich, dass bei klinischen Studien zu Arzneimitteln, deren Marktzulassung beantragt werden soll (Arzneimittelstudien) die Prüfberichte über Verträglichkeit, Wirkung und Nebenwirkungen der einzelnen teilnehmenden Probanden die identifizierenden Merkmale wie die Namensinitialen, das Geschlecht, das vollständige Geburtsdatum und die ethnische Zugehörigkeit enthielten. Damit war es in den Studienzentren einfach, Prüfberichte und Meldungen über unerwünschte Ereignisse zusammenzuführen. Gleichwohl waren durch diese Daten die Betroffenen noch leicht identifizierbar, sodass sowohl die Datenschutzbeauftragten von Bund und Ländern als auch die überwiegende Zahl der Ethikkommissionen ein solches Vorgehen nicht als – gesetzlich vorgeschriebene - Pseudonymisierung bewerteten.

Die Datenschutzgesetze verstehen unter „Pseudonymisieren“ das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen; dieses Kennzeichen soll die Bestimmung des Betroffenen ausschließen oder zumindest wesentlich erschweren

Die getroffenen Aussagen zu den derzeit zwischen Datenschützern, Ethik-Kommissionen und Sponsoren von klinischen Arzneimittelprüfungen laufenden Auseinandersetzungen um den erforderlichen Grad der Pseudonymisierung von erhobenen Probanden-/Patientendaten sind richtig. Die restriktive Einschätzung des Berliner Beauftragten für Datenschutz und Informationsfreiheit (keine Verwendung von Namensinitalien, komplettem Geburtsdatum, Geschlecht und ethnischer Zughörigkeit, stattdessen Benutzung eines anderen frei generierten Kennzeichens) entspricht der Praxis der Ethik-Kommission des Landes Berlin bei deren ethischer Bewertung von klinischen Prüfungen mit Arzneimitteln..

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

(§ 4 Abs. 2 Nr. 8 BlnDSG; § 3 Abs. 6 a BDSG). Die Namensinitialen, das komplette Geburtsdatum, das Geschlecht und die ethnische Zugehörigkeit werden dem keinesfalls gerecht. In den Jahresberichten 2002[81] und 2005[82] sind wir auf die Problematik eingegangen.

§ 4 Abs. **3** Nr. 8 BlnDSG

Dies ist ein Konsens zwischen den Datenschutzbeauftragten von Bund und Ländern, da faktisch alle Dateien über Personen nach Namen, Geburtsdatum und Geschlecht aufgebaut sind und sich allein daraus eine besondere Gefahr bei der Nutzung der Namensinitialen ergibt.

Nunmehr schreibt das Arzneimittelgesetz (AMG) in § 40 verbindlich vor, dass bei allen Meldungen und Datenübermittlungen im Rahmen klinischer Studien die Daten zu pseudonymisieren sind (§ 40 Abs. 2 a Nr. 1 c) und d) AMG). Dies betrifft auch Meldungen über unerwünschte Ereignisse bei der Prüfung des Arzneimittels an den Sponsor (zumeist das forschende Pharmaunternehmen) sowie die zuständige Bundesoberbehörde, die solche Meldungen an eine europäische Datenbank weiterzuleiten hat. Insbesondere bei schwerwiegenden Nebenwirkungen ist hier ein sehr enger zeitlicher Rahmen gesetzt. Wenn beispielsweise ein Hausarzt noch während einer Studie oder nach einer Studie solche Nebenwirkungen bemerkt, sendet er eine entsprechende Meldung an den Sponsor und die Bundesoberbehörde. Dies erfolgt spontan, d. h. nicht im Rahmen des vorgeschriebenen geordneten Studienablaufs. Der Arzt gibt dann zumeist die Namensinitialen und das Geburtsdatum sowie das Geschlecht des Betroffenen an. Mitunter erfolgen die Meldungen auch mit Klarnamen. Für die vorgeschriebenen Meldungen über Nebenwirkungen von zugelassenen Arzneimitteln schreibt das Gesetz – im Gegensatz zu den klinischen Studien vor Zulassung – nicht ausdrücklich eine Pseudonymisierung vor (§ 63 b AMG).

§ 40 Abs. 2 a Nr. **1 b),** c) und d) AMG

Als wir diese Problematik im Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten von Bund und Ländern berieten, legten uns Vertreter eines forschenden Pharmaunternehmens und des Verbandes der forschenden Arzneimittelhersteller die Problematik aus deren Sicht dar. Sie erläuterten, dass eine starke Pseudonymisierung der eigentlichen Studienunterlagen und Protokolle die Zuordnung von Spontanmeldungen erheblich erschweren, wenn nicht sogar unmöglich machen und zu schwer aufzuklärenden Doppelmeldungen führen würde. Zumindest die Nutzung des kompletten Geburtsdatums und des Geschlechts sei erforderlich. Unsere gegenwärtige Position hingegen ist, dass bei den Phasen der klinischen Forschung, an denen nur wenige Patienten beteiligt sind (Phasen I und II), dieses Problem nicht auftreten dürfte. Ob für die Forschung in der Phase III, wenn mehrere Tausend

[81] vgl. 4.5.1
[82] vgl. 4.6.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

erkrankte Probanden an solchen Studien beteiligt sind, das Argument der forschenden Pharmaunternehmen greift, muss weiter geprüft werden. Unsere Behörde wird dies mit den in Berlin ansässigen Pharmaunternehmen beraten und ggf. auch vor Ort prüfen.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit berücksichtigt nicht die Praxis der lokalen Verteilung von Sponsoren, Leitern von klinischen Prüfungen und Prüfstellen in Deutschland bei multizentrischen klinischen Prüfungen. Diese sind bundesweit verstreut und die Auswahl der Prüfstellen sowie des Leiters der klinischen Prüfung durch den Sponsor richtet sich vor allem nach deren fachlicher Eignung. Der Sitz des Sponsors ist nachrangig. Entscheidend für die Zuständigkeit einer nach Landesrecht gebildeten Ethik-Kommission für die Gesamtbewertung einer multizentrischen klinischen Prüfung (einschl. des Umgangs mit personenbezogenen Daten) ist der Sitz des Leiters der klinischen Prüfung. Das Problem der Pseudonymisierung kann also wegen dieser Vernetzung nur bundeseinheitlich übergreifend gelöst werden. Die Beratung mit in Berlin ansässigen Pharmaunternehmen kann daher nur dem gegenseitigen Informationsaustausch dienen. Entscheidungen sind von den Datenschutzbeauftragten des Bundes und der Länder für Deutschland insgesamt und einheitlich zu fällen. Erst dann kann der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Einhaltung der festgelegten Regelung im Land Berlin überprüfen, ggf. auch vor Ort bei Sponsoren, Leitern von klinischen Prüfungen oder einzelnen Prüfstellen im Land Berlin.

Es müssen Wege gefunden werden, um auch bei verzweigter und vielschichtiger Arzneimittelforschung die Datenflüsse so zu gestalten, dass die Identität des Patienten nicht mit einfachen Mitteln bestimmt werden kann.

6.1.2 *Gewebeproben* für die Forschung

National und international lagern in Pathologieinstituten Millionen von Proben, die sich jedoch für die Forschung gegenwärtig nur schwer erschließen lassen. Eine Vernetzung der Informationen über die Proben gibt es bislang nicht. Ein solches Projekt hat das Deutsche Ressourcenzentrum für Genomforschung (RZPD) in Berlin in Angriff genommen.

Die Proben sind aus dem Behandlungszusammenhang oder bei der Leichenschau entstanden. Sie sind natürlich nicht anonym oder pseudonym. Deshalb wird im jeweiligen Pathologieinstitut eine zweite Datenbank (Inhouse-Forschungsdatenbank) aufgebaut. Die Informationen über die einzelnen Proben sind hier pseudonymisiert abgelegt. Die vorhandenen Informationen aus der *Forschungsdatenbank* werden in regelmäßigen Abständen an die Datenbank des RZPD übertragen, allerdings ohne das Pseudonym. Die Datensätze erhalten also nur eine temporäre Kennung. Außerdem ist für die RZPD-Datenbank noch erkennbar, aus welchem Pathologieinstitut die Proben stammen. Durch die ständige Aktualisierung der anonymen RZPD-Datenbank erhält also ein Datensatz mit jeder Datenlie-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ferung eine andere Nummer. Diese Datenbank ist somit nur noch geeignet, statistische Auswertungen durchzuführen. Akkreditierte Forscher können unter verschiedenen Sicherheitsvorkehrungen aus diesen Daten statistische Auswertungen abrufen. Sie erhalten damit beispielsweise die Information, dass in dem Pathologieinstitut A 25 entsprechende Proben, im Pathologieinstitut B 14 gesuchte Proben vorliegen. Der Forscher kann dann mit dem Pathologieinstitut in Kontakt treten und nach entsprechender vertraglicher Regelung beispielsweise Teile dieser Proben oder andere Informationen über die Proben erhalten. Diese Informationen sind wiederum pseudonymisiert.

Die RZPD/CRIP-Datenbank zeigt beispielhaft, wie am Anfang noch personenbezogene medizinische Informationen über ein mehrstufiges Verfahren in anonyme statistische Auswertungen umgewandelt werden und diese für konkrete Forschungsvorhaben wiederum erschlossen werden können.

6.1.3 „Beforschung“ jugendlicher Intensivtäter

Die Landeskommission Berlin gegen Gewalt hat vor dem Hintergrund mehrerer von Jugendlichen begangener Kapitalverbrechen damit begonnen, die Kommunikation zwischen den beteiligten Einrichtungen (Jugendhilfe, Schule, Schulpsychologischer Dienst, Gericht, Staatsanwaltschaft, Polizei, Sozialpsychiatrischer Dienst sowie Kinder- und Jugendpsychiatrie) auf Schwachstellen hin zu untersuchen. Ziel ist es, die Zusammenarbeit dieser Einrichtungen in schwierigen Fällen zu verbessern. Zu diesem Zweck sollen die Akten einer begrenzten Anzahl jugendlicher Intensivtäter, die in der Untersuchungshaft sitzen oder bereits verurteilt sind, analysiert werden. Die Landeskommission bat uns um Unterstützung bei diesem Vorhaben.

Das Vorhaben der Landeskommission führt zu einer Auswertung von sensitiven Informationen über die Untersuchungshäftlinge oder Strafgefangenen, die dem gesteigerten Sozialdatenschutz nach dem Kinder- und Jugendhilferecht, aber auch besonderen Schweigepflichten etwa der Schulpsychologen unterliegen. Es besteht deshalb kein Zweifel daran, dass eine Auswertung aller Akten zu diesen Jugendlichen deren informierte Einwilligung voraussetzt. Die beteiligten schweigepflichtigen Personen müssen von den Betroffenen explizit von ihrer *Schweigepflicht* entbunden werden. Dies muss auf freiwilliger Grundlage geschehen, der Betroffene darf also keinerlei Nachteile erfahren, wenn er einer Auswertung seiner Akten nicht oder nicht vollständig zustimmt.

Die betroffenen Jugendlichen müssen auch darüber aufgeklärt werden, dass sich im Fall ihrer Einwilligung aus den zusammengezogenen Verwaltungsvorgängen möglicherweise Anhaltspunkte für weitere Straftaten ergeben können, die nach dem Legalitäts-

Der Senat vertritt die Auffassung, dass es angesichts des allgemein geltenden Legalitätsprinzips, bei welchem es sich um eine Verpflichtung der Strafverfolgungsbehörde handelt, die verfassungsrechtlich durch den Gleichheitssatz nach Artikel 3 Abs. 1 Grundgesetz

prinzip von den Justizbehörden verfolgt werden müssen. Außerdem sollten die beteiligten öffentlichen Stellen (z. B. die Jugendämter) gerade bei Betroffenen mit Migrationshintergrund, die nicht ausreichend Deutsch verstehen, dafür Sorge tragen, dass ihnen die Bedeutung der Einwilligungserklärung durch einen Dolmetscher vermittelt wird.

Die Landeskommission Berlin gegen Gewalt hat entsprechend unserem Hinweis Einwilligungserklärungen entwickelt, die von den Betroffenen unterzeichnet wurden. Allerdings wurde unsere Empfehlung nicht umgesetzt, dass den Jugendlichen die Konsequenzen ihrer Einwilligung im Zusammenhang mit dem Legalitätsprinzip erläutert werden. Dies wird bei künftigen entsprechenden Fallanalysen zu beachten sein.

Das legitime Interesse des Staates, mögliche Kommunikationsdefizite im Zusammenhang mit jugendlichen Intensivtätern durch Auswertung der Akten aller beteiligten Behörden festzustellen und zu beheben, lässt sich nur in der Weise befriedigen, dass die betroffenen Jugendlichen nach umfassender Information der Auswertung ihrer Akten zustimmen. Falls sie diese Zustimmung verweigern, dürfen ihnen keine Nachteile entstehen.

vorgegeben ist und für die keine gesetzliche Belehrungspflicht besteht, und des Auftrages der von der Landeskommission Berlin gegen Gewalt eingesetzten Arbeitsgruppe, der darin bestand, das institutionelle Handeln der an der Bearbeitung einzelner Fälle von „Intensivtätern“ beteiligten Institutionen zu untersuchen, keinerlei Veranlassung gab, die in die Akteneinsicht Einwilligenden rechtskräftig Verurteilten ausdrücklich darüber aufzuklären, dass es möglicherweise rein theoretisch zu weiteren Strafverfolgungsmaßnahmen kommen könnte, wenn Anhaltspunkte für das Vorliegen eines bis dahin unberücksichtigten Strafverdachts bekannt würden. Abgesehen davon wurden die Betroffenen bzw. ihre gesetzlichen Vertreter umfassend sowohl über die Bedeutung und den Umfang der Erklärung selbst, als auch über den Sinn und Zweck der o.g. Arbeitsgruppe ausführlich belehrt.

6.2 Statistik

6.2.1 Noch vier Jahre bis zur *Volkszählung* 2011

Die Bundesregierung hat im Spätsommer des Jahres 2006 einen Beschluss gefasst, in dem die Grundpositionen für die Teilnahme Deutschlands an der EU-Zensusrunde 2010/2011 festgelegt sind.

Die Erhebung soll sich im Wesentlichen auf Daten stützen, die bei Behörden bereits vorhanden sind. Dies sind im Einzelnen die Melderegister, die Dateien der Bundesagentur für Arbeit und Personaldateien zu Beamten und Richtern, die über ein bundesweit aufzubauendes Register der bewohnten Adressen zusammengeführt werden sollen. Seit dem Jahresbericht 1996 berichteten wir kontinuierlich über die Suche der Statistik nach neuen Methoden und dabei aufgetretenen datenschutzrelevanten Problemen[83] („Volkszählung 2001, 2002, 2003 ...?“).

Mit dem *Zensustest* im Jahre 2001 wurde die grundsätzliche Machbarkeit eines weitgehend auf Register gestützten Zensus nachgewiesen. Allein mit den damals erprobten Methoden können jedoch keine zuverlässigen amtlichen Einwohnerzahlen gewonnen werden. Es ist daher vorgesehen, den registergestützten Teil mit einer direkten Befragung einer Stichprobe von unter 10 % der Bevölkerung zu ergänzen. Die Stichprobe soll außerdem zur Erhebung von Merk-

Der Entwurf des Zensusvorbereitungsgesetzes 2011 (ZensVorbG 2011) wird auf der 853. Sitzung des Bundesrat-Innenausschusses am 26. April 2007 behandelt (Drucksache 222/07). Bereits im Vorfeld haben die Länder in ihren Stellungnahmen zum Referentenentwurf des BMI auf verschiedene datenschutzrechtliche Notwendigkeiten bei der Übermittlung der jeweils geforderten Merkmale hingewiesen.

Im Rahmen der Sitzung des Bundesrat-Innenausschusses ist jetzt zu prüfen, inwieweit die erforderlichen Aspekte des Datenschutzes im Entwurf des ZensVorbG 2011 berücksichtigt sind, insbesondere auch mit Fokus auf den Grundsatz der Trennung von Statistik und Verwaltung. Grundsätzlich sind entsprechende Regelungen in den Gesetzentwurf aufgenommen worden. In § 11 - Geheimhaltung soll mit dem Verweis auf § 16 Bundesstatistikgesetz deutlich gemacht werden, dass bei der Vorbereitung des registergestützten Zensus die Regeln der statistischen Geheimhaltung und damit auch des Datenschutzes gelten und beachtet werden müssen und

[83] JB 1996, 4.5.3

malen und Bevölkerungsgruppen genutzt werden, die nicht in Registern enthalten sind (z. B. Daten zur Bildung und erwerbsstatistische Daten für Selbständige). Diese Direktbefragung mit Kenntnis der Betroffenen dürfte datenschutzrechtlich wenig Probleme aufwerfen.

Anders verhält es sich jedoch beim Aufbau eines Registers der bewohnten Adressen. Hier sollen, bereits im Jahr 2007 beginnend, die Adressdaten der Landesvermessungsämter (einschließlich der geografischen Koordinaten von Gebäuden) mit den Adressdaten aller Melderegister sowie der Bundesagentur für Arbeit zusammengeführt werden. Im Ergebnis entstünde je Land ein Register der bewohnten Adressen, das als Organisationsinstrument des Zensus der Steuerung des Ablaufs der postalischen Gebäude- und Wohnungszählung, der Zusammenführung der verschiedenen Datenquellen und als Auswahlgrundlage für die Stichprobe dient. Die Bundesregierung hat erkannt, dass es allein für diese Vorbereitung des künftigen Zensus eines Gesetzes bedarf. Noch nicht abschließend diskutiert ist der Weg der Bereinigung des Adressregisters. Über die weiteren Nutzungsmöglichkeiten des im Rahmen des Zensus als Organisationsdatei genutzten Adressregisters und über den Aufbau eines fortschreibungsfähigen Gebäude- und Wohnungsregisters hat die Diskussion erst begonnen. Durch das Zusammenführen der verschiedenen Daten kann es also sein, dass bei der Bundesagentur Adressen geführt werden, die in den Melderegistern nicht vorhanden sind. Das Bereinigungsverfahren setzt nun voraus, dass die das Melderegister führende Behörde Kenntnis über Differenzen im Adressmaterial von der amtlichen Statistik zurückerhält. Inwieweit dabei der datenschutzrechtlich entscheidende Grundsatz der Trennung der Statistik vom Verwaltungsvollzug aufrechterhalten wird, bleibt zu prüfen.

In die Vorbereitung der Zählung sollen auch Forscher einbezogen werden, die in der Lage sind, aufgrund einer Unterstichprobe von Adressdaten, jedoch ohne Namen der Einwohner, Grundsätze und Instrumente für die parallel zum registergestützten Zensus notwendige unmittelbare Bevölkerungsbefragung (als Stichprobe, s. o.) zu erarbeiten. Auch dies sollte im Rahmen des bald zu erlassenen Zensusvorbereitungsgesetzes rechtlich eindeutig geklärt werden.

Auch bei einem registergestützten Zensus mit ergänzender Stichprobe ist strikt auf die Einhaltung der Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts von 1983 zu achten.

6.2.2 Ausstattungsvorsprünge Berlins – „Arm, aber sexy“

Bekanntlich hat das Bundesverfassungsgericht am 19. Oktober 2006 ein für Berlin schwieriges Urteil gesprochen. Berlin kann in absehbarer Zeit nicht mer auch in § 13 - Datenübermittlungen soll die Regelung in Absatz 2 sicherstellen, dass bei den Datenübermittlungen die Anforderungen des Datenschutzes beachtet werden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

höhten Sonderzuwendungen des Bundes oder des Länderfinanzausgleichs zum Abbau seiner Schulden rechnen. Das Bundesverfassungsgericht stellte fest, dass bei den sog. Ausstattungsvorsprüngen Berlins gegenüber Hamburg zu berücksichtigen ist, dass ein erheblicher Teil der Mehrausstattung auf Personalausgaben beruht, die kurzfristig in einem nur sehr begrenzten Umfang reduziert werden können.

Ein Instrument, insbesondere um die mittelfristige Personal- und Personalkostenplanung zu unterstützen, ist das Gesetz über die Statistik der Personalstruktur und Personalkosten im unmittelbaren Landesdienst. Wir berichteten darüber in der Vergangenheit[84]. In diesem Gesetz wurde festgelegt, dass eine abgeschottete Statistikstelle zu schaffen ist, die ein im Gesetz festgeschriebenes Konzept „Datenschutz durch Technik“ durchsetzt. Auch hier ist wiederum ein durchdachtes und nicht triviales Konzept der Pseudonymisierung der Ausgangspunkt[85]. Seit Inkrafttreten des Gesetzes im Dezember 2004 arbeitet die Statistikstelle am Aufbau der zentralen Personalstrukturdatenbank und konnte nach erfolgreichen Probeläufen mit fiktiven Daten im vergangenen Jahr im Rahmen des Pilotbetriebes mit Echtdaten folgende Fortschritte erreichen:

- Voraussetzung für die Aufnahme des Pilotbetriebes war die Erfüllung der datenschutzrechtlichen Anforderungen, insbesondere die Erstellung verfahrensspezifischer und infrastruktureller Sicherheitskonzepte. Diese Konzepte sind in ihren wesentlichen Elementen umgesetzt worden.

- Zwischen dem Start des Pilotprojektes mit Echtdaten der Senatsverwaltung für Finanzen im November 2005 und einem Neustart 2006 galt es, verschiedene Anpassungsprobleme zu lösen. Datenschutzrechtlich relevant war vor allen Dingen die Beseitigung von Doppelungen nach dem Pseudonymisierungsprozess. Schrittweise wurden der Automatisierungsgrad des Gesamtverfahrens erhöht und die Prozesse beschleunigt. Im Jahre 2006 wurden zusätzlich die Datensätze von zwei Bezirksämtern, des Polizeipräsidenten und der Senatsverwaltung für Bildung, Jugend und Sport einbezogen.

- Um auch, wie im Gesetz zugelassen, historische Daten einzuspeichern und damit schnellstmöglich Entwicklungen abzubilden, wurden diese rückwirkend bis Januar 2005 erhoben. Um die Dimension zu verdeutlichen: Für die gegenwärtig über 81.000 Personen umfasst eine monatliche Datenlieferung etwa 3,8 Millionen Datensätze. Die historische Datenlieferung für diese Verwaltungen umfasste ca. 54 Millionen Datensätze. Nunmehr sind erste Bewertungen

[84] JB 2002, 4.5.3; JB 2003, 4.5.2; JB 2004, 4.5.2
[85] JB 2005, 3.4

der Datenqualität möglich.

- Auch die Auswertungskomponente wurde erheblich verbessert. So können jetzt die Auswertungen unter strikter Sicherung der Pseudonymisierung in verblüffender Geschwindigkeit vorgenommen werden. Die Statistikstelle sichert bei jeder ihrer Auswertungen das Statistikgeheimnis, sodass kein Personenbezug herstellbar ist. Außerdem sind, wie im Gesetz gefordert, Sichten auf den Gesamtdatensatz und damit universelle Auswertungen nicht möglich. Das System sichert bei der Auswertung, dass - wie vom Gesetz vorgegeben - nur jeweils zwei der sieben Auswertungskomplexe miteinander kombiniert werden können.

Eine noch für 2007 ausstehende Forderung des Gesetzes ist das Ersetzen der Dienstanweisung für den Probebetrieb durch eine Verwaltungsvorschrift, die u. a. die Befugnisse und Pflichten der Statistikstelle und ihrer Mitarbeiter hinsichtlich der technisch-organisatorischen und personellen Abschottung verbindlich regelt.

Insgesamt sind die Voraussetzungen geschaffen, dass die Personalstrukturdatenbank in absehbarer Zeit als eines der modernsten statistischen Instrumente unter Einbeziehung modernster Techniken zur Sicherung des Datenschutzes ihren Echtbetrieb in der ersten Stufe mit monatlich laufenden Datenlieferungen aufnimmt. Damit können unter Wahrung der statistischen Geheimhaltung Daten über die im unmittelbaren Landesdienst Beschäftigten dem Abgeordnetenhaus, dem Senat, den Behörden des Landes, den Beschäftigtenvertretungen, den Gewerkschaften und Berufsverbänden sowie der Öffentlichkeit bereitgestellt werden.

6.3 Schule

6.3.1 *Sprachlerntagebuch* – Note: ungenügend!

Die Senatsverwaltung für Bildung, Jugend und Sport hat ein "Sprachlerntagebuch für Kindertagesstätten" als "Handreichung für Erzieherinnen und Erzieher" herausgegeben. Es ist im Jahr 2004 entwickelt und in 75 Kindertagesstätten von Berlin im I. Halbjahr 2005 erprobt worden. Seit Sommer 2006 wird es in allen Kindertagesstätten Berlins verwendet. Mit dem Sprachlerntagebuch sollen während der gesamten Zeit, die das Kind in der Kindereinrichtung verbringt, regelmäßig der Sprachstand und die Fähigkeit des Kindes, mit seiner Umwelt zu kommunizieren, dokumentiert werden. Das Tagebuch konzentriert sich auf den Erwerb der deutschen Sprache. Gegebenenfalls sollen aus den Feststellungen Förderansätze für die Kinder abgeleitet werden.

Datenschutzrechtlich problematisch an diesem gut gemeinten Vorhaben ist schon die Bezeichnung „Sprachlerntagebuch“. In der Einleitung werden die Kinder

Der Begriff „Sprachlerntagebuch“ wurde gewählt, um den individuellen Bezug jedes einzelnen Kindes herauszustellen, dessen Spracherwerb darin dokumentiert

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

persönlich angesprochen: „Du erhältst von Deiner Erzieherin jetzt ein eigenes *Tagebuch*. Dabei wird der Begriff des Tagebuchs, dem das Kind bei dieser Gelegenheit wohl zum ersten Mal begegnet, geradezu pervertiert. Denn es dient nicht der Aufnahme höchstpersönlicher, intimer Aufzeichnungen, die ein Mensch ihm anvertraut, sondern es soll neben eigenen Beobachtungen, Schreibversuchen und Bildern des Kindes auch Ergebnisse von Interviews enthalten, die Erzieherinnen mit dem Kind führen und sie dort festhalten. Das „Sprachlerntagebuch“ soll also gerade nicht (mit Ausnahme des ersten Teils) vertraulich behandelt, sondern von den Erzieherinnen, Eltern und später sogar den Schullehrern gelesen und genutzt werden. Wie soll ein junger Mensch den strikt vertraulichen Charakter eines Tagebuches verstehen lernen, wenn er als erstes in der Kindertagesstätte diesem „Sprachlerntagebuch“ begegnet?

Das Sprachlerntagebuch ist in vier Teile gegliedert. Der erste Teil beinhaltet Fragen zum „Kennenlernen“ des Kindes und seiner Familie. In einem Gespräch zwischen Leiter/in oder Erzieher/in und den Eltern sollen neben wichtigen Informationen wie Notfallnummern, Allergien usw. überwiegend personenbezogene Fragen zum Kind und seiner Familie beantwortet werden. Die Antworten werden mit den Eltern gemeinsam dokumentiert. In den weiteren Teilen des Buches wird die Entwicklung des Kindes von dem/der jeweiligen Erzieher/in beschrieben. Diese Eintragungen werden hauptsächlich aufgrund von Gesprächen, den sog. "Interviews", mit den Kindern vorgenommen.

wird und mit dem es täglich umgeht. Die Bezeichnung „Tagebuch“ wird nicht immer im Zusammenhang mit einer verschlossenen „geheimen“ Aufzeichnung verwendet, sondern in Pädagogik, Literatur, Seefahrt etc. schon seit alters her als Mittel zur Kommunikation und als ein Instrument des Transfers verwendet. Unter den Bezeichnungen „blogg“ und „weblog“ werden im Internet öffentliche online Tagebücher geführt. Auch die Polizei verwendet den Begriff Tagebuch seit Jahrzehnten, um ihre Tätigkeitsberichte zu sammeln. Jeder, der an einem Verkehrsunfall beteiligt ist, erhält von der Polizei deshalb eine Tagebuch-Nummer, mit deren Hilfe später bei Bedarf das Aktenzeichen der Polizei oder Staatsanwaltschaft ermittelt werden kann. Die Behauptung der angeblichen Pervertierung des Begriffs des „Tagebuchs“, unter dem offenbar ausschließlich ein privates intimes Tagebuch verstanden wird, ist deshalb nicht nachvollziehbar.

Es handelt sich beim Sprachlerntagebuch (der Sprachdokumentation nach § 13 KitaFöG) um ein pädagogisches Instrument, das den Erzieherinnen und Erziehern, dem Kind selbst und seinen Eltern Erkenntnisse über den Entwicklungsstand und die Entwicklungsschritte beim Spracherwerb bringen und in der Kindertagesstätte die Entwicklung gezielter individueller Förderansätze unterstützen soll. Mit der Aufnahme in eine Kindertagesstätte übertragen die Eltern bzw. Erziehungsberechtigten für die Dauer der Anwesenheit die Aufgaben der Betreuung, Erziehung und Bildung ihrer Kinder auf das Personal der Einrichtung. Diese Aufgaben erfordern Kenntnisse über das Kind, seine Entwicklung und sein familiäres Umfeld, um sie erfüllen zu können. Diese Angaben, die im ersten Teil verzeichnet werden, können ihrer Art nach nur bei den Eltern erhoben werden.

Alles, was im zweiten Teil des Sprachlerntagebuches mit den Kindern, Erzieher(innen) und Eltern beobachtet und dokumentiert wird, ist Grundlage für die weiteren Entwicklungsgespräche mit den Eltern über ihr Kind. Mit den Eltern gemeinsam werden bei Bedarf weitere entwicklungsfördernde Schritte besprochen und umgesetzt. Die Kritik offenbart ein erstaunliches Fehlen jeglicher Vorstellung von der alltäglichen Realität des Zusammenlebens mit kleinen Kindern: Bei der Beurteilung der möglichen Brisanz von Informationen, die die Erzieher(innen) beim Gespräch und Malen im Sprachlerntagebuch erlangen, ist zu bedenken, dass Kinder auch ohne dieses pädagogische Mittel in vielerlei Weise unaufgefordert Einzelheiten aus ihrem Familienleben in Gesprächen, Bildern oder Rollenspielen mitteilen. Dass kleine Kinder Ereignisse anders wahrnehmen als Jugendliche oder Erwachsene und sie auch anders darstellen, ist allen in einer Kindertageseinrichtung Tätigen bewusst.

Die Informationen im Sprachlerntagebuch gehen nicht über den in Kindertagesstätten üblichen Informationsstand hinaus, sondern standardisieren sie, um sie zur

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Sprach- und Bildungsförderung nutzbar zu machen. Im Ausnahmefall wird in gesonderten Vereinbarungen mit den Eltern bei zu schützenden Informationen über das Kind oder aus dem familiären Bereich für besondere Vertraulichkeit in der Einrichtung bzw. gegenüber Erzieher(innen) gesorgt, weil es sonst im täglichen Umgang der Erzieher(innen) mit dem Kind keine festzulegenden Grenzen gibt. Es ist der Professionalität der Pädagog(inn)en überlassen zu erkennen, wenn eine Situation entsteht, die besonderen Schutz von intimen Informationen erfordert.

Für die Implementierung des Instrumentes ist die Handreichung für Erzieher(innen) entwickelt worden, die Informationen zur Entwicklung, Bewertungen und Anleitungen zur Anwendung und zur Zusammenarbeit mit den Eltern enthält. Darin wird darauf hingewiesen, dass das Sprachlerntagebuch für Kind und Eltern jederzeit zugänglich sein soll, damit es als lebendiges gemeinsames Instrument in die pädagogische Praxis der Kindertagesförderung Eingang findet. Die Formulierung in der Handreichung, wonach der erste Teil wegen der vertraulichen Informationen getrennt aufbewahrt werden „sollte“, ist allerdings unglücklich, so dass die Gefahr bestand, dass er als Empfehlung unbeachtet bleibt.

Die Einführung des Berliner Bildungsprogramms und des Sprachlerntagebuches wird durch umfängliche Fortbildungsveranstaltungen unterstützt. Der Implementierungsprozess für die pädagogische Praxis ist noch nicht abgeschlossen. In diesen Veranstaltungen wird auf die ordnungsgemäße Verwahrung der nicht öffentlich zugänglichen Teile der Sprachlerntagebücher ausdrücklich hingewiesen.

Die Bücher sind Eigentum des Kindes und seiner Eltern und am Ende der Kita-Zeit „an das Kind und die Eltern“ vollständig zu übergeben. Auf der vorderen Innenseite des Sprachlerntagebuches wird im Grußwort des Senators eindeutig gesagt: „Am Ende der Kita-Zeit Ihres Kindes in der Einrichtung wird es Ihnen ausgehändigt“ Das Interesse der Schule wird dabei nicht ignoriert, sondern den Eltern mitgeteilt, dass die Tagebücher für die Lehrer(innen) der Grundschule wertvolle Hinweise geben können. Die Entscheidung, ob das Tagebuch - vollständige oder nach Entfernung einzelner Seiten aus dem Ringbuch – in der Grundschule genutzt werden soll, bleibt aber bei den Eltern.

Da der erste Teil vertrauliche Informationen enthält, empfiehlt die Senatsverwaltung, diesen getrennt vom Sprachlerntagebuch aufzubewahren und ihn bei Übergabe an das Kind und die Eltern wieder beizufügen.

Nach der Ausgabe des Sprachlerntagebuchs hat sich eine große Zahl betroffener Eltern an den Berliner Beauftragten für Datenschutz und Informationsfreiheit gewandt und zu Recht auf gravierende datenschutz-

Erstaunlicherweise sind bei der Senatsverwaltung für Bildung, Wissenschaft und Forschung keine begründeten Beschwerden über Fehlverhalten im Zusammenhang mit dem Sprachlerntagebuch eingegangen. Die

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

rechtliche Mängel hingewiesen. Pointiert ausgedrückt ermöglicht das Sprachlerntagebuch eine weitgehende Ausforschung von Kindern über ihre persönlichen und familiären Verhältnisse. So sollen sie z. B. über die in der Familie gesprochene Sprache Auskunft geben.

Informationen zum ersten Teil des Buches werden über Gespräche mit den Kindern eingeholt. Die Angaben werden dabei unkritisch in das Tagebuch aufgenommen, es wird nicht zwischen den Aussagen jüngerer und älterer Kinder differenziert. Vor allem werden die Eltern nicht über die *Freiwilligkeit* der Führung des Sprachlerntagebuches für ihr Kind informiert. Große Unsicherheit besteht bei den Eltern hinsichtlich des Umgangs mit den erhobenen Daten. Im Vorwort des Dokuments befinden sich dazu keine Erläuterungen. Die Eltern haben uns geschildert, besonders große Unklarheiten bestünden zu der Frage, wofür die Daten verwendet würden, ob eine Weitergabe und wie die Auswertung der Daten erfolge.

Aus den Eingaben geht hervor, dass auch die Leiter/innen und Erzieher/innen der Kindereinrichtungen nicht in ausreichendem Maße auf die Führung eines Tagebuches und den Umgang mit den dort erhobenen Daten vorbereitet wurden. So wird uns berichtet, die Tagebücher liegen vollständig, also ohne Ausgliederung des ersten Teils mit den personenbezogenen Eintragungen, in den Räumen der Kindertagesstätten aus. Die Bücher seien somit offen für jede Person einsehbar.

Schließlich, so berichten Eltern, seien sie aufgefordert worden, das Sprachlerntagebuch in der zukünftigen

fünf Eingaben von Eltern hatten nur Fragen nach dem Zweck einzelner Daten zum Inhalt, die in allen Fällen ausgeräumt werden konnten. Um die Fehler, die es nach den Erfahrungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit in einzelnen Einrichtungen bei der Handhabung der Sprachlerntagebücher dennoch gegeben zu haben scheint, wurde vorsorglich in einem Schreiben an alle Einrichtungsträger klargestellt, dass

1) die persönlichen und zum Teil vertraulichen Informationen des ersten Teils getrennt aufbewahrt und erst zur Übergabe an die Eltern wieder in das Sprachlerntagebuch eingefügt werden sollen,
2) die Verwahrung dieser Informationen in einem nicht frei zugänglichen Raum, so dass er nur Befugten [also den Eltern, der Einrichtungsleitung und dem/der zuständigen Erzieher(in)] auf Anforderung z. B. von der Leiterin ausgehändigt werden kann, unbedingt zu gewährleisten ist,
3) das Sprachlerntagebuch beim Ausscheiden des Kindes aus der Kindertagesstätte an das Kind und dessen Eltern oder sonstige Erziehungsberechtigte heraus zu geben ist. Ausdrücklich wird nochmals erläutert, dass es der Entscheidung der Eltern überlassen ist, ob und in welcher Form sie das Sprachlerntagebuch später der Lehrerin oder dem Lehrer der Schulanfangsphase in der Grundschule übergeben und dies die Kindertagesstätte den Eltern nur empfehlen kann.

Der kommenden Auflage des Sprachlerntagebuchs wird außerdem ein ausführliches Informationsschreiben an alle Eltern beigelegt werden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Schule ihres Kindes abzugeben. Welchem Zweck dies dienen soll, bleibt unklar. Den Eltern wird auch nicht freigestellt, das Sprachlerntagebuch nicht der Schule zu übergeben, wenn sie z. B. verhindern wollen, dass ihr Kind durch bestimmte Informationen im Sprachlerntagebuch vorbelastet wird und diese Vorbelastung während seiner schulischen Laufbahn nicht mehr abschütteln kann.

Ein „Sprachlerntagebuch“, das die Ausforschung von Kindern über ihre Familiensituation ermöglicht, verstößt gegen die Persönlichkeitsrechte von Kindern und Eltern. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat deshalb die erheblichen datenschutzrechtlichen Mängel gegenüber der zuständigen Senatsverwaltung für Bildung, Wissenschaft und Forschung beanstandet und sie zur Beseitigung der datenschutzrechtlichen Mängel aufgefordert.

6.3.2 Der Albtraum einer zentralen Schülerdatenbank

Der „Pisa-Schock“ treibt immer neue Blüten. Die Kultusministerkonferenz verfolgt bereits seit längerem das Vorhaben, eine über den gesamten Bildungsweg eines Kindes bzw. Jugendlichen konstante Schüleridentifikationsnummer zu vergeben, um damit eine bundesweite Schülerdatenbank aufzubauen. Dieser Plan wurde erst 2006 in der Öffentlichkeit bekannt und stieß dort zu Recht auf scharfe Kritik.

In dieser *Schülerdatenbank* würden sich dann Daten von ca. 12 Millionen Schülern befinden. Solche Datenbanken – sind sie erst einmal vorhanden – wecken bekanntlich eine ganze Reihe von Begehrlichkeiten. Fraglich ist, ob es mit dem allgemeinen Persönlichkeitsrecht vereinbar ist, Daten so zu speichern, dass gerade die für die Persönlichkeitsentwicklung entscheidenden Jahre mit all ihren Wirrungen, Hochs und Tiefs dauerhaft abgebildet werden können. Die Ausbaufähigkeit einer solchen Datenbank zur lückenlosen Abbildung des Einstiegs ins Berufsleben über Lehre, Arbeitslosigkeit oder Studium liegt auf der Hand.

Mit Datensammelwut und entsprechendem Aktionismus auf Mängel, Probleme und Defizite in den Schulsystemen zu reagieren ist nicht überzeugend. Selbst wenn eine solche bundesweite Datenhaltung zügig eingeführt werden sollte, würden Ergebnisse, die den gesamten Schulverlauf der Schüler abbilden und somit die Probleme des Schulsystems unzweideutig belegen können, erst nach 2020, womöglich erst 2022 oder 2023 vorliegen.

Die Berliner *Schülerstatistik* ist bis zum laufenden Schuljahr eine klassenbezogene Datenerhebung. Pro Klasse wird erhoben, wie viele Jungen, wie viele Mädchen, wie viele Kinder und Jugendliche ausländischer Staatsbürgerschaft in welchen Unterrichtsfächern oder mit welchem Förderbedarf unterrichtet

In der Bildungspolitik ist das Interesse groß. Die ursprünglichen Pläne, über eine eindeutige Schüler-ID den Bildungsgang der Schülerinnen und Schüler verfolgen zu können, wurden in Berlin auch auf Grund der noch notwendigen Festlegungen zur Einhaltung gesetzlicher und datenschutzrechtlicher Bestimmungen zurückgestellt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

werden. Die Personenbeziehbarkeit ist schon bei der Erhebung wesentlich erschwert, da jeder für eine Klasse erzeugte Datensatz nur selten Merkmale enthält, die bloß auf einen oder zwei Schülerinnen oder Schüler zutreffen.

Diese bisherige Praxis schöpft jedoch nicht den geltenden Rechtsrahmen in Berlin aus. Bereits 1992, als die aufgrund der Schulgesetzänderung notwendige Schuldatenverordnung vorbereitet wurde, trug die Senatsschulverwaltung den Wunsch vor, die Schülerstatistik nicht mehr klassenbezogen, sondern auf den einzelnen Schüler bezogen durchzuführen. Dies war für uns nachvollziehbar, da die Auswertung auf klassenbezogene Summendaten beschränkt und ihre Kombination über die Schule und den Schultyp nicht möglich war. In die Schuldatenverordnung von 1993 wurde die Befugnis für die Senatsschulverwaltung aufgenommen, zweimal jährlich Einzelangaben der Schüler, aber ohne die Merkmale Name, Tag der Geburt und genaue Anschrift zu erheben. Schulnummer, Klassen- und Kursbezeichnung durften zur Zuordnung der Einzelangaben verwendet werden. Unmittelbar identifizierende Daten sollten nicht erhoben werden. Auch war festgelegt worden, dass diese Einzelangaben der statistischen Geheimhaltung und den Regelungen des Landesstatistikgesetzes unterliegen und die Organisationseinheit, die mit der Schulstatistik beauftragt ist, organisatorisch, personell und räumlich von anderen Organisationseinheiten zu trennen ist. Es waren also alle rechtlichen Rahmenbedingungen für die Erfassung von Einzeldaten geschaffen.

Von dieser rechtlichen Möglichkeit, die nunmehr auch im Berliner Schulgesetz verankert ist, hat die Senatsschulverwaltung in den vergangenen 13 Jahren keinen Gebrauch gemacht. Die Gründe mögen vielfältig gewesen sein. Ab dem Schuljahr 2008/2009 sollen jetzt die Voraussetzungen für die Erhebung von Schülerindividualdaten im Rahmen der Schulstatistik geschaffen werden. Die Senatsschulverwaltung informierte uns 2005 über das Bestreben, die Schulstatistik auf Länderebene bei der Erhebung eines sog. Kerndatensatzes, d. h. länderübergreifend übereinstimmender Inhalte der zu erhebenden Merkmale, zu vereinheitlichen. Im Sommer dieses Jahres teilte uns die Senatsschulverwaltung mit, dass vorgesehen ist, die Schuldatenverordnung an die im Kerndatensatz der Kultusministerkonferenz vorgegebenen Merkmale anzupassen. Daher wurden durch eine Änderung der Schuldatenverordnung als schülerbezogene Merkmale der Schulstatistik das Geburtsland, bei einem nichtdeutschen Geburtsland das Jahr des Zuzuges, die Kommunikationssprache in der Familie und ein Hinweis auf die Befreiung von der Verpflichtung zur Zahlung eines Eigenanteils bei Lernmitteln neu aufgenommen. Dieses letzte Merkmal ist von einer besonderen Sensitivität, da es Rückschlüsse auf die soziale Bedürftigkeit der Familie erlaubt. Daher dürfen diese Daten nur vom Schulleiter

Der in der Vergangenheit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit erfolgte Austausch von Informationen und Dokumenten im Zusammenhang mit der geplanten Schülerindividual-Statistik, zeugt von den Bemühungen des Senats, die von der Kultusministerkonferenz geforderten datenschutzrechtlich nicht abgesicherten Beschlüsse mit einer vertretbaren Lösung für Berlin unter Einhaltung des Datenschutzgesetzes zu vereinbaren.
Die Umsetzung der Schülerindividualstatistik für Berlin ist in Vorbereitung und wird im Schuljahr 2008/09 in Form einer Online-Erfassung eingeführt. Ob das Merkmal Lernmittelbefreiung in die Schülerindividualstatistik mit aufgenommen werden kann, ist noch nicht abschließend geklärt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

oder einem ausschließlich mit dieser Aufgabe beauftragten Mitarbeiter, der ohnehin davon Kenntnis hat, erhoben werden. 2006 wurden aber auch diese neuen Merkmale mit der Schülerstatistik noch klassenbezogen erhoben.

Keinesfalls ist es mit den jetzigen rechtlichen Regelungen für die Berliner Schulstatistik vereinbar, ein landesweites einheitliches Schülerregister mit einer dauerhaften Schüleridentifikationsnummer aufzubauen und damit die Grenzen zwischen Statistik und Verwaltungsvollzug zu sprengen. Zwar soll der Schüler durch eine eindeutige Nummer innerhalb der Schule gekennzeichnet werden. Diese Nummer darf aber bei Schulwechsel nicht mit übermittelt werden. Die neue Schule vergibt für den Schüler dann eine neue Nummer. Damit ist zwar die Entwicklung eines Schülers im Rahmen einer Schule statistisch nachvollziehbar, jedoch nicht über den Rahmen der Schule hinaus. Diese Zuordnungsnummer als Hilfsmerkmal im statistischen Sinne, ihre Bildung und Verwendung sowie möglicherweise andere Fragen der Organisation der Schülerindividualstatistik in Berlin bedürfen sicherlich noch einer weiteren Anpassung der Schuldatenverordnung im Rahmen ihrer für 2007 vorgesehenen Überarbeitung.

Mit der Erstellung eines Sicherheitskonzeptes der Senatsverwaltung für Bildung, Wissenschaft und Forschung in Zusammenarbeit mit dem IT-Dienstleistungszentrum Berlin (ITDZ), wurden Risiken untersucht und Maßnahmen festgelegt, um im Jahr 2008/09 eine Basis zu schaffen, die eine vereinfachte Schülerindividual-Statistik ermöglicht, die auf einer pseudonymisierten Datengrundlage (nur schulinterne Schüler-ID, die im Statistik-Bereich gelöscht wird) auskommt und trotzdem qualitativ wertvollere statistische Auswertungen zulässt, als es in der Vergangenheit möglich war. Solange die datenschutzrechtlichen Belange in Berlin und bundesweit ungelöst sind, ist weder die Einführung einer berlinweiten Schüler-ID noch ein elektronischer Datenexport der Individualdaten an die Kultusministerkonferenz vorgesehen.

Die Berliner Schulverwaltung arbeitet parallel zu den bisherigen Konzepten der Kultusministerkonferenz an einem Vorschlag, wie durch die Lieferung aufbereiteter statistischer Daten an ein festzulegendes statistisches Amt eine solide und valide bundesweite Schülerstatistik organisiert werden kann, aber ein bundesweites Schülerregister mit einer dauerhaften Schüleridentifikationsnummer vermieden wird.

Die Kultusministerkonferenz berät gegenwärtig noch über mögliche Varianten u.a. auch über einen Vorschlag der Senatsverwaltung für Bildung, Wissenschaft und Forschung.

Damit befindet sich die Berliner Schulverwaltung mit ihrer Schulstatistik in Übereinstimmung mit uns und der Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder[86]. Der Konferenz erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen Bildungsregisters in Anbetracht der aus den verschiedenen wissenschaftlichen Untersuchungen wie PISA vorliegenden Ergebnisse nicht dargetan. Sie fordert nachdrücklich einen Verzicht auf die Identifikationsnummer. Das Erhebungsprogramm der Schulstatistik ist auf Statistikzwecke zu beschränken. Bei der Datenverarbeitung ist nach dem Gebot der Trennung von Verwaltungsvollzug und Statistik zu verfahren.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass Schulministerien in mehreren Ländern das bisherige datenschutzrechtlich bedenkliche Konzept eines bundesweiten personenbezogenen Bil-

[86] „Keine Schülerstatistik ohne Datenschutz“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 19

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

dungsregisters nicht mehr weiterverfolgen. Sie streben dies auch als Ergebnis der mit der Kultusministerkonferenz zu führenden Gespräche an.

6.3.3 Der Schüler als Fernsehstar – Serie „S.0.S.“ Hilferuf aus dem Klassenzimmer“

Durch Beschwerden und die Berichterstattung in der Tagespresse[87] haben wir davon erfahren, dass in der Pommern-Oberschule in Berlin-Charlottenburg die mehrteilige Fernsehreportage "S.O.S. Schule – Hilferuf aus dem Klassenzimmer" gedreht worden war. Es wurden unter aktiver Mitwirkung von Schülern, deren Erziehungsberechtigten und Lehrern der Schule dokumentarische Filmbeiträge mit Szenen aus dem allgemeinen Schulleben, dem Unterricht in den Klassen, Beratungen im Lehrerkollegium und der familiären, häuslichen und sozialen Situation einzelner Schülern erstellt, zweimal im ZDF ausgestrahlt und im Internet zum Abruf bereitgestellt. Die Pommern-Oberschule teilte uns dazu mit, dass die Gesamt- und die Schulkonferenz dem Filmprojekt zugestimmt habe. Von der Schulaufsicht sei eine Drehgenehmigung erteilt worden. Die betroffenen Lehrer hätten ihr Einverständnis erklärt. Von allen Eltern und Schülern würden dem ZDF Einverständniserklärungen vorliegen. Zwei Schüler, von denen diese Erklärungen nicht hätten eingeholt werden können, seien durch entsprechende Materialbearbeitung nicht gezeigt worden.

Das Bildmaterial zu den Filmbeiträgen der Serie "S.O.S. Schule - Hilferuf aus dem Klassenzimmer" enthält zweifelsfrei personenbezogene Daten von Lehrkräften und Schülern der Pommern-Schule, deren Erziehungsberechtigten und sonstigen Dritten. Ein Teil der Filmaufnahmen dokumentiert, unter aktiver Beteiligung von Vertretern der Schulleitung und/oder Lehrkräften, den Ablauf und den Inhalt schulischer Veranstaltungen (Klassenunterricht, pädagogische Einzelgespräche, Beratungen über Erziehungs- und Ordnungsmaßnahmen). Für diesen Teil der Bildaufnahmen handelte die Pommern-Schule - ungeachtet einer vorhandenen Drehgenehmigung für das ZDF durch die Schulaufsicht - als datenschutzrechtlich verantwortliche Stelle.

Durch die aktive Teilnahme der Schule an den *Filmaufnahmen* hat diese personenbezogene Daten der Betroffenen an einen Dritten (die Filmproduktionsfirma) übermittelt. Betroffene sind hier nicht nur die Lehrkräfte, Erziehungsberechtigten und die sich aktiv be-

Der im Jahresbericht geschilderte Vorfall war bereits Gegenstand eines Schriftwechsels mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit im November 2006 / Februar 2007. Kern der Beanstandung des Beauftragten ist der Umstand, dass die an der Fernsehübertragung Beteiligten zwar (möglicherweise) gegenüber dem ZDF eine Einwilligungserklärung abgegeben haben, nicht aber gegenüber der Schule. Zumindest sind dort schriftliche Einwilligungserklärungen nicht (mehr) auffindbar. Auch wenn bisher nicht eindeutig erkennbar ist, ob die Beanstandung des Berliner Beauftragten für Datenschutz und Informationsfreiheit auf die konkrete Beschwerde eines Betroffenen zurückgeht oder er die Veröffentlichung in der Tagesspresse zum Anlass für Nachforschungen genommen hat, wurde dieser Vorfall zum Anlass genommen, ein Informationsschreiben nebst einem Muster für die erforderlichen Einwilligungserklärungen an die Betroffenen zu geben, damit in künftigen Fällen auch den datenschutzrechtlichen Anliegen der Betroffenen in ausreichendem Maße Rechnung getragen werden kann.

Der Bericht, die Analyse und die Bewertung des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu der o.g. Fernsehserie entspricht den Gegebenheiten. Die Drehgenehmigung ist durch die regionale Schulaufsicht ausgesprochen worden. Die Einwilligung

[87] Tagesspiegel v. 4. Mai 2006, S. 9

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

teiligenden Schüler, sondern auch die Schüler, die erkennbar im Hintergrund der Filmaufnahmen (z. B. im Unterricht) zu sehen sind. Eine derartige Übermittlung von personenbezogenen Daten ist nach § 64 Abs. 4 Satz 2 Nr. 1 Schulgesetz (SchulG) nur mit *Einwilligung* der Gefilmten zulässig. Durch die Aufnahme und Ausstrahlung des Bildmaterials wird zudem erheblich in die Persönlichkeitsrechte der betroffenen Schüler, insbesondere in ihr Recht am eigenen Bild, eingegriffen. Für die Datenübermittlung durch die Schule an die Filmgesellschaft ist daher in jedem Einzelfall die Einwilligung der Erziehungsberechtigten bzw. des einwilligungsfähigen Schülers erforderlich. Die Einwilligung ist von der Daten verarbeitenden Stelle (hier: der Pommern-Schule) schriftlich und im Vorfeld der Filmaufnahmen bei den Betroffenen einzuholen. Dabei ist den Betroffenen das Recht einzuräumen, dass sie der Weitergabe ihrer Daten an die Filmgesellschaft jederzeit widersprechen können.

Die Schule kann sich ihrer Verantwortung für die – teilweise minderjährigen – Schüler und für die Lehrer nicht dadurch entziehen, dass sie es einer Fernsehanstalt oder Produktionsfirma überlässt, entsprechende Einwilligungserklärungen einzuholen. Das Abgeordnetenhaus von Berlin hat bereits 2004 in einem Beschluss[88] die Pflicht der öffentlichen Verwaltung betont, bei Film- und Fernsehaufnahmen im Zusammenhang mit Verwaltungstätigkeiten den Schutz des Persönlichkeitsrechts der Bürgerinnen und Bürger sicherzustellen. Auf die Einhaltung dieser Rechtspflichten wurden die Senats- und Bezirksverwaltungen in der Vergangenheit mehrfach vom Regierenden Bürgermeister von Berlin[89] hingewiesen. Sie gelten in besonderem Maße in Schulen, wo Schülerinnen und Schüler zwar häufig geneigt sein werden, sich an „*Reality TV*"-Sendungen zu beteiligen, ohne allerdings die Tragweite dieser Entscheidung immer zu überblicken. Was einmal in die Medienöffentlichkeit und insbesondere ins Internet gelangt ist, kann nicht mehr „widerrufen" werden.

Die Pommern-Schule konnte die erforderlichen schriftlichen Einwilligungserklärungen nicht vorlegen. Selbst wenn die Betroffenen Erklärungen gegenüber der Filmgesellschaft abgegeben haben (was wir nicht überprüfen konnten), wäre dies für die datenschutzrechtliche Bewertung unbeachtlich, zumal die Schulleitung nicht geltend gemacht hat, dass sie den Inhalt dieser Einwilligungserklärungen geprüft und sich zu eigen gemacht hat. Im Ergebnis bleibt festzustellen, dass die Übermittlung der personenbezogenen Daten durch die Pommern-Schule an die Fernsehproduktionsfirma ohne datenschutzrechtliche Einwilligung der Betroffenen und damit rechtswidrig erfolgt ist.

der Gefilmten ist im Vorfeld versehentlich von dem Fernsehproduktionsteam eingeholt worden.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die Übermittlung personenbezogener Daten - hier: Filmaufnahmen von Schülerinnen und Schülern - zu Recht beanstandet. Die Schulleiter/innen der Region Charlottenburg-Wilmersdorf sind im vergangenen Jahr auf die datenschutzrechtlichen Bestimmungen hingewiesen worden, dass sie im Hinblick auf die Erteilung der Drehgenehmigung und die schriftliche Einwilligungserklärung der Gefilmten im Vorfeld der Aufnahmen <u>*selbst*</u> handeln müssen.

[88] Beschluss v. 13. Mai 2004, JB 2004, Anhang 1

[89] vgl. Rundschreiben v. 17. Mai 2004 und 9. Februar 2006

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat das Vorgehen der Leitung der Pommern-Schule dementsprechend beanstandet.

Beabsichtigt eine Schule, personenbezogene Daten (z. B. über Schüler) aus schulischen Veranstaltungen an Medien- und Filmgesellschaften zu übermitteln, hat sie als Daten verarbeitende Stelle bei den Betroffenen zur Wahrung der Persönlichkeitsrechte und zur Einhaltung des Datenschutzes zuvor selbst eine informierte schriftliche Einwilligung einzuholen.

6.3.4 Wenn Lehrer zu Hilfspolizisten werden - Einziehung und Inhaltskontrolle von *Schüler-Handys*

Die Mutter eines Schülers beschwerte sich bei uns darüber, dass Lehrkräfte an der Schule ihres Sohnes die Handys einer ganzen Klasse eingezogen und deren gespeicherte Inhalte kontrolliert hätten. Von der Schule wurde dieser Sachverhalt bestätigt. Ziel der Aktion sei es gewesen, Video mit gewaltverherrlichenden bzw. nationalsozialistischen Inhalten zu finden und von den Schülern löschen zu lassen. Auf den Handys von vier Schülern seien entsprechende Videos gefunden worden. Diese seien gelöscht und mit den Schülern darüber konstruktive Gespräche geführt worden. Eine Bestrafung der Schüler sei nicht erfolgt.

Handys sind Multifunktionsgeräte mit einer Vielzahl von technisch unterstützten Möglichkeiten. Die Geräte werden von ihren Besitzern zur Kommunikation, Adressverwaltung, Kalenderführung, Archivierung von Nachrichten, Texten, Videos usw. genutzt. Im Zusammenhang mit diesen Funktionen sind in den Geräten erhebliche Mengen von personenbezogenen Daten über den Besitzer oder Dritte gespeichert. Diese Daten ermöglichen nicht nur Rückschlüsse auf die Nutzungsprofile zu den einzelnen (z. B. Kommunikations-)Funktionen. Sie enthalten auch Angaben (z. B. durch elektronische Tagebuchführung) über sonstige persönliche oder sachliche Verhältnisse der Betroffenen.

Durch die Suche nach den verbotenen Videos in den Inhaltsdaten der Handys haben die Lehrkräfte einen Teil dieser Daten zwangsläufig zur Kenntnis genommen. Datenschutzrechtlich ist dies als Erhebung von personenbezogenen Daten zu bewerten.

Nach § 64 Abs. 1 SchulG dürfen Schulen die personenbezogenen Daten von Schülern und deren Erziehungsberechtigten erheben, die zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen "schulbezogenen" Aufgaben erforderlich sind. Gemeint ist hier nicht der allgemeine Auftrag der Schule zur Bildung und Erziehung, sondern die "schulbezogenen" Aufgaben, die (im engeren Sinne) mit der Organisation und Durchführung des Schulbetriebes verbunden sind.

Der Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit stellt zu Recht darauf ab, dass es nach den derzeitigen gesetzlichen Bestimmungen Lehrkräften nicht erlaubt ist, die auf Schülerhandys gespeicherten Daten ohne deren Einwilligung zu durchsuchen. Liegen Anhaltspunkte für ein strafrechtlich relevantes Verhalten vor, so kann die Lehrkraft nach § 62 Abs.2 Nr. 6 SchulG das Handy einziehen und der herbeigerufenen Polizei übergeben, die dann weitere Maßnahmen veranlassen kann. Da der Senatsverwaltung für Bildung, Wissenschaft und Forschung über das benannte Beispiel hinaus keine weiteren Vorfälle mehr bekannt wurden, wird davon ausgegangen, dass es sich bei dem geschilderten Vorfall um einen Einzelfall handelt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Kenntnisnahme und Erhebung der umfangreichen, zum Teil vertraulichen Handydaten war für keine der in § 64 Abs. 1 SchulG genannten "schulbezogenen" Aufgaben erforderlich. Die pädagogische Aufbereitung des Themas "Gewaltverherrlichung" hätte auch ohne die Überführung von "Einzeltätern" erfolgen können.

Bei den Inhaltsdaten von Schüler-Handys handelt es sich um zum Teil vertrauliche Daten des Besitzers und Dritter. Diese Daten dürfen Lehrkräfte einer Schule nur mit Einwilligung der Betroffenen erheben. Beim Verdacht der Begehung von Straftaten hat eine Mitteilung an die Strafverfolgungsbehörden zu erfolgen, die dann entsprechende Durchsuchungen der Inhaltsdaten von Handys vornehmen können.

6.3.5 Der Schul*pranger* - vom "Steckbrief" bis zum "pädagogischen" Aushang über Versäumnisse

Immer wieder beschäftigen uns Fälle, in denen Schüler und ihr Verhalten in der Öffentlichkeit bloßgestellt werden.

Ein besonders schwerer Fall ereignete sich an der Friedrich-Bergius-Oberschule. Dort hatte eine Schülerin während ihres freiwilligen Cafeteria-Dienstes einen Schokoriegel entwendet. Die Verfehlung der Schülerin wurde vom Schulleiter u. a. mit einem lebenslangen Cafeteria-Verbot bestraft. Zur Durchsetzung des Verbotes wurde das "Urteil" zusammen mit einem Lichtbild der Schülerin an der Tür zur Cafeteria öffentlich ausgehängt.

Eine derartige Übermittlung von personenbezogenen Schülerdaten in Form eines "Steckbriefes" und die damit verbundene Prangerwirkung in der Öffentlichkeit sind datenschutzrechtlich natürlich unzulässig. Der Schulleiter erklärte, nachdem wir ihn in einem Gespräch auf die Unzulässigkeit der Maßnahme hingewiesen hatten, dass ein anderer Weg gefunden werde, um die aufsichtführenden Lehrer über das Cafeteria-Verbot zu informieren.

Das vom Berliner Beauftragten für Datenschutz und Informationsfreiheit in seinem Jahresbericht zu Recht kritisierte Beispiel ist nicht Ausdruck einer generellen Situation an Berliner Schulen, sondern es handelt sich nach Rücksprache mit der Schulaufsicht um einen Einzelfall, der so an anderen Schulen bisher nicht aufgetreten ist. Bei der Entscheidung der Schulleitung oder der Lehrkraft, welche pädagogischen Maßnahmen nach einem Vorfall zu ergreifen sind, müssen im Rahmen des weiten pädagogischen Ermessens auch die datenschutzrechtlichen Belange des Einzelnen berücksichtigt und in die Abwägung eingestellt werden. Maßgeblich ist auch hier der Einzelfall. Ohne eine genaue Kenntnis der Gesamtumstände des Einzelfalls verbietet sich eine Beurteilung der von der Schulleitung oder der Lehrkraft durchgeführten Maßnahme.

Eltern haben sich mehrfach bei uns darüber beschwert, dass Lehrer die Versäumnisse von Schülern (z. B. Hausaufgaben nicht gemacht, sich nicht am Unterricht beteiligt, Arbeitsmaterial zu Hause vergessen) auf großen Listen im Klassenzimmer aushängen würden.

Nach § 1 Schulgesetz (SchulG) ist es die Aufgabe der

Der Vorfall (Diebstahl eines Schokoriegels und die fol-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Schule, alle wertvollen Anlagen der Kinder und Jugendlichen zur vollen Entfaltung zu bringen und ihnen ein Höchstmaß an Urteilskraft, gründliches Wissen und Können zu vermitteln. Den Lehrkräften wird durch § 67 Abs. 2 SchulG die Aufgabe zugewiesen, die ihnen anvertrauten Schüler in eigener pädagogischer Verantwortung im Rahmen der Bildungs- und Erziehungsziele und der geltenden Vorschriften und Konferenzbeschlüsse zu unterrichten, zu erziehen, zu beurteilen, zu bewerten, zu beraten und zu betreuen. Somit hat die Schule nicht nur den Auftrag, Wissen zu vermitteln, sondern auch die Verpflichtung, pädagogisch auf die ihr anvertrauten Kinder und Jugendlichen einzuwirken und ihnen eine Einordnung der eigenen Leistung zu ermöglichen.

Wird die Verantwortung der Lehrer nicht durch Beschlüsse der Gesamtkonferenz eingeschränkt, bleibt es ihrem pädagogischen Ermessen überlassen, in welcher Weise sie z. B. den Schülern die Noten bekannt geben. Danach kann es z. B. im Einzelfall durchaus zulässig sein, die Noten aller Schüler im Rahmen des Unterrichts vor der Klasse bekannt zu geben und mithilfe eines Notenspiegels die Eltern über die leistungsmäßige Einordnung ihrer Kinder zu informieren. Zu beanstanden ist hingegen das Vorgehen eines Lehrers, der bewusst nur die (schlechten) Noten einzelner Schüler verliest oder anderweitig Schülern bzw. Eltern mitteilt, um diese einzelnen Schüler vor den Mitschülern bloßzustellen.

Die pädagogischen Freiräume des Lehrers enden dort, wo gezielt oder unbewusst Maßnahmen mit Prangerwirkung ergriffen werden. Vergleichbares gilt auch für die Ausstellung von benoteten Schülerarbeiten oder Aushänge über deren Leistungen in den Klassenräumen. Handelt es sich dabei um Räumlichkeiten, die auch von Dritten genutzt werden oder für diese (z. B. Reinigungskräfte usw.) zugänglich sind, werden durch die Aushänge personenbezogene Daten der Schüler an diese Dritten übermittelt. Handelt es sich bei diesen Dritten um schulfremde Personen (z. B. Eltern, Unterrichtsbesucher usw.), ist eine derartige Übermittlung nach § 64 Abs. 4 SchulG grundsätzlich nur mit Einwilligung der Betroffenen zulässig. Die Reichweite der Einwilligung endet auch hier dort, wo mit der Datenübermittlung gezielt oder unbewusst eine Prangerwirkung einhergeht. Von einer derartigen Prangerwirkung ist jedenfalls dann auszugehen, wenn sich der (öffentliche) Aushang in Form eines negativen Rankings ausschließlich auf die Versäumnisse einzelner Kinder (z. B. Hausaufgaben nicht gemacht, mangelhafte Unterrichtsbeteiligung usw.) bezieht.

Die Bekanntgabe von benoteten Schülerarbeiten an schulfremde Dritte oder deren Ausstellung in Räumen (z. B. Klassenzimmer), die schulfremden Personen zugänglich sind, ist grundsätzlich nur mit Einwilligung der Betroffenen zulässig. Aushänge mit Angaben über Versäumnisse einzelner Schüler sind dagegende Maßnahme) haben an der Friedrich Bergius-Oberschule stattgefunden. Die zuständige Schulaufsicht der Außenstelle Tempelhof-Schöneberg hat sofort nach Bekannt werden den Vorfall mit der Schulleitung erörtert und zu einer veränderten Maßnahme gebracht: Es wurde - wie zutreffend dargestellt - ein anderer Weg gefunden, um die aufsichtsführenden Lehrkräfte über das Cafeteria-Verbot der Schülerin zu informieren.

Die im Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit genannten Begriffe „Steckbrief“ und „Prangerwirkung“ sind fehlerhaft. Diese Begriffe entstammen einem anderen Kontext, der durch diese Maßnahme nicht gegeben war.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

gen in jedem Fall unzulässig.

6.3.6 Der Dauerbrenner! - Zulässigkeit der Weitergabe von Elterndaten durch die Schule an Dritte

Immer wieder beschweren sich empörte Eltern bei uns darüber, dass ihre Adressdaten auf einem Elternabend, an dem sie nicht teilgenommen haben, von dem/der Klassenlehrer/in oder den Elternvertretern - zumeist als Teil einer Adressenliste - an die anderen Eltern in der Klasse weitergegeben wurden. In einem besonderen Fall wurde dadurch die geschützte - im Einwohnermelderegister gesperrte - Adresse von Pflegeeltern eines Kindes, das von seinem leiblichen Vater mehrfach misshandelt worden war und vor diesem versteckt lebt, mit nicht absehbaren Folgen für das Kind Dritten bekannt gegeben.

Die Schule darf personenbezogene Daten an private Dritte grundsätzlich nur mit Einwilligung der Betroffenen übermitteln (§ 64 Abs. 4 SchulG). Dies gilt auch für die Weitergabe von Adressdaten der Eltern, Erziehungsberechtigten usw. an Dritte (z. B. die Miteltern einer Klasse). Im Regelfall tragen sich die anwesenden Eltern eines Elternabends in eine Liste ein, die dem Zweck der gegenseitigen Kontaktaufnahme dient. Dabei können sie entscheiden, ob und welche Angaben (Anschrift, Telefonnummer, E-Mail-Adresse usw.) sie machen. Die Daten von abwesenden Eltern dürfen nicht ohne deren Einwilligung nachgetragen und verteilt werden.

Anders verhält es sich bei den Daten über die gewählten Elternvertreter. Nach § 10 Abs. 7 Schuldatenverordnung darf die Schule deren Namen, Anschriften und Telefonnummern an die Erziehungsberechtigten der Schüler ihrer Klasse und an den Vorsitzenden der Gesamtelternvertretung (GEV) weitergeben. Die Weitergabe von Namens- und Adressdaten der Elternvertreter bzw. der gewählten GEV-Mitglieder an Dritte (z. B. interessierte Erziehungsberechtigte) außerhalb des Klassenverbandes ist nicht ausdrücklich geregelt. Allerdings bestimmt § 122 Abs. 2 Satz 1 SchulG, dass Lehrkräfte, Schüler sowie Erziehungsberechtigte Einsicht in die Sitzungsprotokolle der Gremien ihrer Schule nehmen können. Diese Protokolle enthalten auch die Namen der anwesenden Mitglieder. Daraus lässt sich ableiten, dass die Schule berechtigt ist, die Namen der GEV-Mitglieder an Dritte (z. B. interessierte Erziehungsberechtigte) weiterzugeben. Eine Herausgabe der privaten Telefonnummern und/oder Privatadressen der gewählten GEV-Mitglieder an Dritte ist dagegen - ohne Einwilligung der Betroffenen - in jedem Fall unzulässig.

Die Schule darf die Adress- und Kontaktdaten von Eltern grundsätzlich nur mit deren Einwilligung an private Dritte weitergeben.

Zu Recht weist der Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit darauf hin, dass personenbezogene Daten, wie z.B. die Adresse, ohne die Einwilligung der Betroffenen nicht gegenüber Dritten bekannt gegeben werden dürfen. Da hierzu in der Praxis noch immer Aufklärungsbedarf besteht, wird im Rahmen der Dienst- und Schulleiterbesprechungen hierzu nochmals eine Information erfolgen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

6.4 Kultur

6.4.1 Städtische *Bibliotheken*: Zögerliche Buchrückgabe – zögerliche Datenlöschung

Ein Berliner war zwar ein fleißiger Leser, jedoch hielt er die Rückgabezeiten der entliehenen Bücher nicht ganz so fleißig ein, wie es von den Bibliotheken vorgeschrieben war. Immer wieder häuften sich Mahn- und Verwaltungsgebühren an, die er dann - oft verspätet - bezahlte. Er beschwerte sich, dass die Gebührendaten nicht unverzüglich nach Bezahlung gelöscht wurden. Er stellte zwar nicht infrage, dass die unbezahlten Mahngebühren bis zum Zeitpunkt der endgültigen Abrechnung gespeichert bleiben durften, jedoch beklagte er sich darüber, dass er sich durch die noch auf seinem Konto ersichtlichen Gebührendaten als säumiger Zahler diskriminiert fühle, obwohl er doch seine Gebühren, wenn auch verspätet, vollständig bezahlt habe.

Wir nahmen die Beschwerde zum Anlass für eine Überprüfung des Verbuchungssystems bei der *Buchausleihe* durch die städtischen Bibliotheken Berlins. Denn nach § 4 Abs. 3 Gesetz über die Datenverarbeitung im Bereich der Kulturverwaltung vom 26. Januar 1993[90] sind Daten der Bibliotheksbenutzer zu löschen, sobald der Grund für ihre Speicherung entfallen ist. In die Überprüfung haben wir eine städtische Bücherei und auch die „Bibliothek auf Rädern“, den Bibliotheksbus, einbezogen. Die Überprüfung verschaffte uns ein Bild über das gesamte Verbuchungssystem, da die Datenverarbeitung der Ausleihe einschließlich aller Gebührenbuchungen für alle städtischen Büchereien im zentralen Rechner der städtischen Bibliotheken (VÖBB) erfolgt.

Die Überprüfung führte unter anderem auch zur Verbesserung hinsichtlich der von uns festgestellten Mängel bei der Gebührenverbuchung. So wurde – im Sinne der Beschwerde des Petenten - die Löschung beglichener Entgeltforderungen den gesetzlichen Erfordernissen des § 4 des Gesetzes über die Datenverarbeitung im Bereich der Kulturverwaltung vom 26. Januar 1993 angepasst. Fehler in der Software, die ein regelmäßiges Löschen beglichener Entgeltforderungen von gekennzeichneten Datensätzen verhinderten, wurden ausgeräumt.

Wir hatten im Zuge der Überprüfung auch festgestellt, dass die Ausweisdaten inaktiver Bibliotheksbenutzer bis dahin unbefristet aufbewahrt worden waren, in einem Fall seit über fünf Jahren. Es konnte aber erfreulicherweise eine Einigung mit der Bibliotheksleitung dahingehend erzielt werden, dass Daten inaktiver Bib-

Der - dank der Intervention des Petenten gefundene - Fehler bezog sich nicht auf alle, sondern nur einen Teil der Gebührenkonten. Der Fehler konnte behoben werden, so dass die Löschung der bezahlten Gebühren nun automatisiert für alle Gebührenkonten erfolgen kann. Die Löschung der mindestens seit zwei Jahren inaktiven Bibliothekskunden ist erfolgt und wird in Zukunft regelmäßig vorgenommen werden. Gemäß Beschluss der Bibliotheksamtsleiterinnen und -leiter betrifft die Genehmigung zur Löschung inaktiver Bibliothekskunden keine Konten mit unbezahlten Gebühren, unabhängig vom Entstehungsdatum des Gebührensatzes.

[90] in der Fassung des Artikels IV des Gesetzes zur Änderung bibliotheksrechtlicher Vorschriften – Bibliotheksrechtliches Änderungsgesetz – BiblÄndG v. 29. September 2004, GVBl., 428, 431

liotheksbenutzer grundsätzlich nach zwei Jahren gelöscht werden. Eine fortdauernde Speicherung der Ausweisdaten bis zu zwei Jahren nach Ablauf der Nutzungsberechtigung halten wir für angemessen, da es auch im positiven Interesse eines „ruhenden“ Bibliotheksbenutzers liegt, ihm das „Wiedereinsteigen“ in die Bibliothekennutzung durch die dann noch mögliche Fortschreibung der Gültigkeit des Ausweises zu erleichtern.

Aufgrund unserer Intervention werden im Verbuchungssystem der öffentlichen Bibliotheken die Daten säumiger Entleiher und inaktiver Benutzer nicht mehr länger als erforderlich gespeichert.

6.4.2 *Ausreiseantrag* und *Rehabilitation* nach dem SED-Unrechts-Regime

Über DDR-Bürger, die ein Ausreiseverfahren eingeleitet hatten, weil sie in der DDR ihre persönlichen Lebensvorstellungen nicht verwirklichen konnten, wurden in den DDR-Behörden „Ausreiseakten“ geführt. Diese Akten bezogen sich bei Familien nicht allein auf die Einzelperson eines Antragstellers, sondern auch auf die Familien in ihrer Gesamtheit, sofern die anderen Familienangehörigen in irgendeiner Weise von der Ausreise betroffen waren. Die hierzu in den Akten dokumentierten und zusammengefassten persönlichen Lebensumstände betrafen also auch die ganz persönliche Situation eines einzelnen Familienmitgliedes oder diejenige von näheren und ferneren Anverwandten und Freunden, die in den Akten auftauchten. Die Ausreiseakten sind im Rahmen der heutigen Rehabilitationsverfahren nach dem SED-Unrechtsbereinigungsgesetz zur Beurteilung der Ausreisegründe und der erlittenen Unrechtssituation unentbehrlich. Da die Akten jedoch Daten auch über die näheren Lebensumstände anderer Mitglieder des Familienverbandes enthalten, wollte das Landesarchiv wissen, ob diese Akten vollständig und ungeschwärzt und/oder nur mit Einverständnis aller anderen Personen, die sich jeweils aus den Akten ergeben, im Rehabilitationsverfahren zur Verfügung gestellt werden dürften.

Das Landesarchiv archiviert die Ausreiseakten ehemaliger Ausreisewilliger aus der DDR. Als Archivgut unterliegen die Akten dem Landesarchivgesetz. Nach § 8 Archivgesetz des Landes Berlin (ArchGB) könnte, vor Ablauf der archivrechtlichen Nutzungssperre bei archivierten personenbezogenen Daten, lediglich mit Einwilligung der Betroffenen Einsicht in deren personenbezogene Daten gewährt werden. Es ging also um die Frage, ob von jedem Familienmitglied oder sonstigen Betroffenen, die in einer Akte erwähnt werden, eine Einverständniserklärung beigebracht werden müsste, um die Nutzung der Ausreiseakten im Rehabilitationsverfahren durch einen anderen Betroffenen möglich zu machen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Unsere Überprüfung ergab, dass das Rehabilitationsverfahren bereichsspezifische Regelungen im Sinne des Datenschutzrechts enthält. Es gibt drei Kategorien der Rehabilitation, die jeweils in unterschiedlichen Gesetzen geregelt sind, nämlich

1. die berufliche Rehabilitation,
2. die verwaltungsrechtliche Rehabilitation,
3. die strafrechtliche Rehabilitation.

Alle Rehabilitationsgesetze enthalten Regelungen, die sich u. a. auch auf das Informationsrecht beziehen und mit denen die Interessenlage der Beteiligten befriedigend gelöst werden kann. Im verwaltungsrechtlichen Rehabilitationsgesetz (VwRehaG)[91] ist eine Regelung zur Verwendung personenbezogener Daten in § 11 VwRehaG enthalten, so auch im beruflichen Rehabilitationsgesetz in § 19 BerRehaG[92] und im strafrechtlichen Rehabilitationsgesetz in § 25 a StrRehaG[93]. Diese im Wesentlichen übereinstimmenden Regelungen lauten, vom verwaltungsrechtlichen Rehabilitationsgesetz, §11 VwRehaG, ausgehend, z. B. wie folgt:

„Personenbezogene Daten aus einem *verwaltungsrechtlichen* Rehabilitationsverfahren dürfen auch für andere Verfahren zur Rehabilitierung, Wiedergutmachung oder Gewährung von Leistungen nach dem Häftlingshilfegesetz soweit erforderlich verarbeitet und genutzt werden."

Die Regelungen lassen erkennen, dass der Gesetzgeber das informationsrechtliche Problem der Datennutzung erkannt hatte und lösen wollte. Die Ausreiseakten entsprachen seinerzeit nicht den datenschutzrechtlichen Geboten des Grundgesetzes und konnten ihnen - systembedingt - nicht entsprechen. Andererseits war es nicht möglich, den gesamten Aktenbestand nach der Wiedervereinigung in eine Übereinstimmung mit dem informationellen Selbstbestimmungsrecht zu bringen und umzuordnen. Deshalb hat der Gesetzgeber, um die Wiedergutmachung und Rehabilitation nicht an etwaigen datenschutzrechtlichen Einwänden anderer Beteiligter scheitern zu lassen, gesetzlich ausdrücklich klargestellt, dass im vorrangigen Interesse der Rehabilitation die Nutzung der in den jeweiligen Unterlagen enthaltenen Daten Mitbetroffener zulässig ist. Diese Befugnis zur Nutzung der ungeschwärzten Ausreiseakten ist jedoch ausdrücklich auf die Rehabilitationsverfahren zu beschränken.

Im Übrigen muss es aber bei den Nutzungsregelungen nach § 8 ArchGB von Berlin bleiben. Es gibt vor Ablauf der Sperrfristen ohne Einverständnis der Betroffenen keinen Zugriff Dritter auf Daten, die in Ausrei-

[91] BGBl I 1997, 1621
[92] BGBl I 1997, 1626
[93] BGBl I 1999, 2665

seakten aufbewahrt werden.

Aus der Systematik der Rehabilitationsgesetze ergibt sich die wertende Entscheidung des Gesetzgebers, dass das Verfahren des einen Rehabilitationsantragstellers nicht durch fehlende Rehabilitationsanträge oder Einverständniserklärungen anderer mitbetroffener Ausreisewilliger behindert werden soll. Vielmehr haben Mitbetroffene die Nutzung der vollständigen Ausreiseakten im übergeordneten Interesse der Rehabilitation eines Antragstellers hinzunehmen.

7 Wirtschaft

7.1 Verkehrsunternehmen

7.1.1 Zusammenarbeit zwischen Deutscher Bahn AG, Inkasso-Unternehmen und Auskunftei

Eine schwangere Bahnfahrerin musste feststellen, dass sowohl der Fahrkartenautomat im Bahnhofsgebäude als auch der auf dem Bahnsteig defekt waren. Da sie schweres Gepäck bei sich hatte, entschied sie sich, die Fahrkarte im Zug zu lösen. Sie meldete sich bei dem Kontrolleur, der ihr mitteilte, dass eine Fahrpreisnacherhebung nicht durchgeführt würde, wenn ihre Angaben richtig seien. Er notierte sich ihren Namen und ihre Anschrift. Trotz dieser Zusage erhielt sie kurze Zeit später ein Schreiben, in dem ein erhöhtes Beförderungsentgelt gefordert wurde. In mehreren Antwortschreiben legte die Betroffene dar, warum der Anspruch ihrer Meinung nach nicht besteht. In zwei Mahnungen der Deutschen Bahn AG sowie zwei weiteren Mahnungen eines eingeschalteten Inkasso-Unternehmens ging man auf ihre Argumente nicht ein. Stattdessen erhielt sie von dem Inkasso-Unternehmen den Hinweis, dass es ihre Daten an eine Wirtschaftsauskunftei übermitteln würde.

Die Weitergabe von Negativdaten an eine Auskunftei (Einmeldung) von einem Inkasso-Unternehmen ist nur unter engen Voraussetzungen gestattet. Sowohl Gläubiger als auch Inkasso-Unternehmen haben die zugrunde liegende Forderung gegenüber dem Schuldner jeweils mindestens zweimal vergeblich schriftlich anzumahnen. Der Schuldner ist darüber zu informieren, dass eine Einmeldung bei einer Auskunftei erfolgt, soweit keine Zahlung innerhalb der gesetzten Frist erfolgt. Diese Formalvoraussetzungen haben die beteiligten Unternehmen eingehalten. Übersehen wurde allerdings, dass nur unbestrittene Forderungen eingemeldet werden dürfen, deren Nichtbegleichung auf Zahlungsunwilligkeit oder Zahlungsunfähigkeit beruht. Selbst wenn die Deutsche Bahn AG und das Inkasso-Unternehmen die Rechtsauffassung der Betroffenen nicht teilten und davon ausgingen, dass ein Anspruch auf ein erhöhtes Beförderungsentgelt besteht, war die Drohung des Inkasso-Unternehmens mit einer

Einmeldung an eine Auskunftei rechtswidrig. Demgegenüber hätten keine Bedenken dagegen bestanden, wenn das Inkasso-Unternehmen die Forderung gerichtlich verfolgt hätte. Auf unsere Empfehlung hin wurde auf die Einmeldung der Daten der Petentin verzichtet.

Inkasso-Unternehmen dürfen nur unbestrittene Forderungen bei Auskunfteien einmelden, die der Schuldner nicht begleichen will oder kann.

7.1.2 Ende einer Firmenehe

Die Deutsche Bahn AG hat mehrere Jahre mit einem Autovermieter eng kooperiert. Der Autovermieter konnte das Buchungssystem der Deutschen Bahn AG mitbenutzen. Die Partnerschaft wurde im Streit beendet, die Deutsche Bahn AG schaltete das Buchungssystem des jetzt mit der Deutschen Bahn AG konkurrierenden Autovermieters ab. Im Anschluss daran hat die Deutsche Bahn AG Kunden des Autovermieters eine E-Mail geschickt und auf den Service ihres Tochter-Unternehmens DB Carsharing hingewiesen.

Die Deutsche Bahn AG hatte für den ehemaligen Partner Kundendaten im Auftrag verarbeitet (§ 11 Bundesdatenschutzgesetz – BDSG). Auftragnehmer dürfen personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Die Deutsche Bahn AG hatte somit nicht das Recht, die personenbezogenen Daten des neuen Konkurrenten für eigene Zwecke zu nutzen. Die Nutzung der E-Mail-Adressen für Werbezwecke verstieß außerdem gegen § 7 Abs. 2 Nr. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Datennutzungen unter Verstoß gegen das UWG sind nach § 4 Abs. 1 BDSG rechtswidrig. Die Deutsche Bahn AG hat den Datenschutzverstoß eingeräumt und will sicherstellen, dass sich ähnliche Vorgänge zukünftig nicht wiederholen.

Auftragsdatenverarbeiter dürfen Daten, die sie von ihrem Auftraggeber erhalten haben, nicht auftragswidrig für eigene Zwecke nutzen.

7.1.3 Nochmals: Gutscheinvergabe bei *Zugverspätungen*

In unserem letzten Jahresbericht[94] haben wir über die Datenerhebung der Deutschen Bahn AG im Rahmen von Gutscheinkarten wegen Zugverspätungen berichtet.

Die Deutsche Bahn AG begründete die Datenerhebung damit, einerseits ein aktives Beschwerdemanagement führen zu wollen und andererseits den Missbrauch mit den Gutscheincoupons verhindern zu müssen. Wir stellten dennoch einen Verstoß gegen § 28

[94] JB 2005, 4.7.1

Abs. 1 Nr. 1 und 2 BDSG fest, da eine Erhebung personenbezogener Daten nur dann zulässig ist, soweit dies zur Missbrauchsbekämpfung erforderlich ist. Es wurde Einvernehmen mit der Deutschen Bahn AG erzielt, dass nunmehr wieder alle Kunden Entschädigungen wegen Zugverspätungen ohne Angabe personenbezogener Daten erhalten, die einen Originaleinzelfahrschein mit einem entsprechenden Vermerk über die Verspätung vorlegen. Die Erhebung von Fahrgastdaten zu Zwecken der Kundenbetreuung ist dagegen zulässig, wenn sich der Kunde ihr durch Widerspruch entziehen kann.

Die Gutscheinkarten werden unverzüglich nach Inkrafttreten einer EU-Verordnung zur Novellierung der Passagierrechte bei der Deutschen Bahn angepasst (ca. 2. Halbjahr 2007). Die Deutsche Bahn AG hat jedoch schon jetzt alle Mitarbeiter im direkten Kundenkontakt auf die geänderte Verfahrensweise hingewiesen.

7.2 Banken und Versicgherungen

7.2.1 Verkauf der Berliner Bank

Im Jahre 2006 wurde die Berliner Bank an die Deutsche Bank verkauft. In dem Bieterverfahren hatten die Interessenten Gelegenheit, sich über die finanzielle Situation des potenziellen Kaufobjekts zu informieren (Due-Diligence-Verfahren). Während dieses Verfahrens wurden die für die Interessenten entscheidungserheblichen Unterlagen in einen sog. „Grünen Raum" gebracht. Anders als im Due-Diligence-Verfahren bei der Bankgesellschaft Berlin[95] *befanden sich im „Grünen Raum" keine Akten, sämtliche Unterlagen waren eingescannt. Die Bieter hatten insbesondere Zugriff auf ausgewählte Kreditakten und andere Portefeuille-Angaben des Unternehmens.*

Während des Bieterverfahrens ist sicherzustellen, dass die Bieter keine personenbezogenen Informationen über die Bankkunden, die auch durch das *Bankgeheimnis* geschützt sind, und über Mitarbeiter der Bank erhalten. Gerade zu diesem Zweck wird der „Grüne Raum" eingerichtet, in den nur anonymisierte Unterlagen gelangen dürfen. Vor Beginn des Bieterverfahrens haben wir in der Bank eine Kontrolle durchgeführt, um zu überprüfen, ob das Anonymisierungsgebot im Bieterverfahren eingehalten wurde.

Bei unserer Kontrolle stellten wir fest, dass fast in jedem Datensegment Anonymisierungen bzw. Schwärzungen versäumt wurden. Bei einigen Verträgen wurden die Namen der Mitarbeiter, die für den Vertragsabschluss verantwortlich waren, nicht geschwärzt. Hierdurch war erkennbar, welcher Mitarbeiter für notleidende Kredite eine Mitverantwortung trägt. Teilweise war der Name des Bearbeiters geschwärzt, dafür

[95] JB 2003, 4.6.1

fehlte aber die Schwärzung bei seinem Vorgesetzten. Die Namen der Personalratsmitglieder wurden in einem Dokument mit Vor- und Zunamen aufgeführt.

Bei laufenden Gerichtsverfahren wurden die beteiligten Rechtsanwälte mit kompletten Namen und Adresse benannt. Soweit die Bank Gutachten in Auftrag gegeben hatte, insbesondere Gutachten zur Bewertung von Grundstücken, wurden die Gutachter nicht nur mit vollem Namen genannt, auch ihre Bankverbindung wurde aufgeführt.

Teilweise wurde versäumt, sogar den Namen und das Geburtsdatum eines Kontoinhabers zu schwärzen. Es wurden auch Eigentümer von Grundstücken namentlich benannt, ebenso Mieter, die in einem bestimmten Projekt wohnen. Insbesondere sind die Mitarbeiter der Bank davon ausgegangen, dass die genaue Anschrift eines Objekts, für das ein Kredit gezahlt wurde, nicht geschwärzt werden muss. Dies ist deshalb unzutreffend, da über das Objekt der jeweilige Kreditnehmer ermittelbar ist, also ein personenbeziehbares Datum vorliegt.

Der Bank wurde aufgegeben, vor Beginn des Bieterverfahrens die Mängel zu beseitigen. Dies wurde von uns in einer Stichprobe überprüft.

Im Due-Diligence-Verfahren ist im Rahmen einer Unternehmensveräußerung sicherzustellen, dass der „Grüne Raum“ keine personenbezogenen Daten enthält.

7.2.2 Rechtswidrige SCHUFA-Abfrage

Bei der Einholung der SCHUFA-Selbstauskunft stellte ein Bürger fest, dass eine Berliner Privatbank seine SCHUFA-Daten abgefragt hatte. Als Grund für die Abfrage hatte die Bank eine Kreditanfrage des Betroffenen angegeben. Der Betroffene beschwerte sich bei der Bank, mit der er zu keinem Zeitpunkt in einer geschäftlichen Beziehung gestanden hatte, insbesondere hatte er keinen Kredit bei der Bank beantragt. Die Bank bedauerte den Vorfall, nannte jedoch keine Gründe für die nicht nachvollziehbare SCHUFA-Abfrage.

Die Berliner Privatbank ist eine Tochtergesellschaft einer Hamburger Bank, die im Rahmen eines Geschäftsbesorgungsvertrages verschiedene Arbeiten ihrer Tochter übernommen hat, so z. B. die Justiziararbeit. Dem Justiziar der Muttergesellschaft wurde die Möglichkeit eingeräumt, über die Berliner Privatbank bei Bedarf Anfragen an die SCHUFA zu stellen.

Unsere Ermittlungen ergaben, dass der Sohn des Petenten in der Hamburger Bank arbeitet. Dieser hatte ein persönliches Interesse an den SCHUFA-Daten seines Vaters, da er in einem Unterhaltsprozess die Interessen seiner Mutter vertrat. Der Verdacht, dass

der Justiziar seinem Arbeitskollegen die Daten beschafft hat, konnte nicht ausgeräumt werden. Seine Einlassung, er habe sich bei einer privaten Rechtsberatung des Sohnes die personenbezogenen Daten des Petenten (einschließlich Geburtsdatum) notiert und dann bei einer vorzunehmenden SCHUFA-Abfrage „die Zettel verwechselt", erscheint wenig glaubhaft. Auch überraschte es, dass die Berliner Privatbank bei einer Kontrolle der Aufsichtsbehörde keine Dokumentation der SCHUFA-Abfrage vorlegen konnte.

Wir haben die Berliner Privatbank aufgefordert, ihr berechtigtes Interesse an SCHUFA-Daten auch dann zu prüfen, wenn ein Mitarbeiter der Muttergesellschaft diese anfordert. Außerdem hat die Bank die Gründe für das Vorliegen eines berechtigten Interesses nach § 29 Abs. 2 letzter Satz BDSG zu dokumentieren. In dem konkreten Fall hätte sich dem für SCHUFA-Abfragen zuständigen Mitarbeiter auch die Frage aufdrängen müssen, wieso bei dem Justiziar der Muttergesellschaft eine Kreditanfrage an seine Bank eingegangen ist.

Die Anforderung von SCHUFA-Daten durch die Muttergesellschaft entbindet eine Bank nicht von der Pflicht, ihr berechtigtes Interesse an der Abfrage zu prüfen und zu dokumentieren.

7.2.3 Eine fingierte Einwilligungserklärung

Die Kunden einer Berliner Versicherung erhielten ein Mitteilungsschreiben, in welchem auf den Zusammenschluss mit einer Bayerischen Versicherungsgruppe hingewiesen und eine überarbeitete Einwilligungsklausel zum Datenschutz beigefügt wurde. Den Kunden wurde mitgeteilt, man werde von der Zustimmung zur Einwilligungsklausel ausgehen, wenn sie nicht widersprächen. Als relevante Änderung wurde insbesondere erwähnt, dass die Vertragsdaten in einem gemeinsamen System zusammengeführt werden und die Berliner Versicherung die Datenverarbeitungssysteme der Bayerischen Versicherungsgruppe mit nutzen wird. Nur in der Einwilligungserklärung, nicht jedoch in dem Anschreiben wurde darauf hingewiesen, dass konzernweite Datenflüsse zum Zwecke der Vertrags- und Leistungsbearbeitung beabsichtigt seien. Gegen die Vorgehensweise der Versicherung sind bei uns zahlreiche Beschwerden eingegangen.

Bei Unternehmenszusammenschlüssen besteht für Versicherungen das Problem, dass die Einholung einer an den neuen Verhältnissen orientierten Einwilligungserklärung bei den Bestandskunden zu Umsetzungsproblemen führt. Die Antwortquote der Kunden ist sehr gering. Aus diesem Grunde besteht bei den Aufsichtsbehörden die grundsätzliche Bereitschaft, die Umsetzung von Firmenzusammenschlüssen mit pragmatischen Lösungen zu unterstützen.

Erste Voraussetzung für die Privilegierung von Daten-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

flüssen bei Unternehmenszusammenschlüssen ist das Vorliegen einer bestehenden rechtswirksamen *Einwilligung*serklärung. Diese kann unter bestimmten Bedingungen um die durch den Zusammenschluss neu entstehenden Datenflüsse erweitert werden, indem die Kunden über die Änderungen informiert werden und ihnen ein Widerspruchsrecht eingeräumt wird. Danach soll durch die Einräumung des „Opt-out-Rechts“ und die fehlende Reaktion des Betroffenen die bestehende Einwilligungserklärung den neuen Gegebenheiten angepasst, also aktualisiert werden. Durch das Schreiben an den Bestandskunden kann aber nicht eine unwirksame Einwilligungserklärung in eine wirksame „umgewandelt werden“.

Die Berliner Versicherung verwendet bei dem Abschluss von Versicherungsverträgen Einwilligungserklärungen, die Teil des Versicherungsvertrages waren, aber im Text nicht besonders hervorgehoben wurden. Damit waren sie nach § 4 a Abs. 1 letzter Satz BDSG i. V. m. § 125 Satz 1 BGB nichtig.

Wir haben die Berliner Versicherung darauf hingewiesen, dass das Schreiben an die Versicherungsnehmer nicht dazu führt, dass der Kunde durch Schweigen in die geplanten Datenflüsse einwilligt. Neben der rechtswidrigen Ursprungseinwilligungserklärung hatte die Versicherung es auch versäumt, ihre Kunden schon im Anschreiben auf die gravierende Änderung der in der Einwilligungserklärung genannten Übermittlungstatbestände hinzuweisen, die über das durch den Zusammenschluss erforderliche Maß deutlich hinausgingen. Falls Versicherungen beabsichtigen, im Rahmen von Unternehmenszusammenschlüssen künftig weitere Datenverarbeitungsprozesse vorzunehmen, in die bislang noch nicht eingewilligt worden ist, so müssen sie in dem Anschreiben an die Versicherungsnehmer in hinreichend deutlicher Form auf die künftigen Änderungen hinweisen. Die Versicherung hat unsere Hinweise zum Anlass genommen, auf die geplanten Datenübermittlungen zu verzichten.

Liegt eine rechtswirksame Einwilligungserklärung vor und wird ein Versicherungsnehmer ausreichend über neu entstehende Datenflüsse informiert, kommt als Rechtsgrundlage für die nicht in der Ursprungseinwilligungserklärung enthaltenen Datenflüsse § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Der Versicherungsnehmer, der trotz ausreichender Informationen auf das ihm eingeräumte Widerspruchsrecht verzichtet, hat keine schutzwürdigen Interessen am Ausschluss der Verarbeitung. Die Übermittlung sensitiver Daten bedarf aber weiterhin einer „normalen Einwilligungserklärung“. Auch unterliegen Mitarbeiter bestimmter Versicherungsunternehmen einer strafbewehrten Schweigepflicht (§ 203 Abs. 1 Nr. 6 StGB).

Auch nach dem Zusammenschluss von Versicherungen gelten die alten Einwilligungserklärungen fort. Nur unter engen Voraussetzungen kann eine Erweite-

rung der ursprünglich vorgesehenen Datenverarbeitungsprozesse bei ausreichender Transparenz und Einräumung eines Widerspruchsrechts akzeptiert werden.

7.2.4 Aktenfund im Mülleimer

Ein Bürger beschwerte sich darüber, dass die auf seinem Nachbargrundstück befindliche Bankfiliale Papiermüll in seinem Mülleimer entsorgt. Darunter befanden sich Kontoauszüge, Kreditanträge und SCHUFA-Anfragen.

Die Überprüfung des Vorfalls ergab, dass die Mitarbeiterin einer beauftragten Reinigungsfirma den Inhalt der Papierkörbe weisungswidrig in die Mülltonnen des Nachbargrundstücks geworfen hat. Dies erschien ihr arbeitssparender als die für die Entsorgung vorgesehene Papiertonne, die aus Gründen des Datenschutzes und zur Verhinderung des Einwurfs von Plastikmüll nur durch einen schmalen Papierschlitz gefüllt werden konnte.

Da die Bank mit dem Reinigungsunternehmen keinen Auftragsdatenverarbeitungsvertrag abgeschlossen hatte, durfte es an der Entsorgung von datenschutzrelevantem Altpapier nicht beteiligt werden. Die Bank hat inzwischen ihr Recycling-Verfahren geändert, zukünftig sind die Bankmitarbeiter selbst verpflichtet, datenschutzrelevantes Papier in der Papiertonne zu entsorgen.

Mitarbeiter von Fremdfirmen dürfen ohne Vorliegen eines Auftragsdatenverarbeitungsvertrages nicht an der Aktenvernichtung beteiligt werden.

7.3 Was wir sonst noch geprüft haben …

7.3.1 Allgemeines Gleichbehandlungsgesetz

Am 18. August 2006 ist nach langen Debatten das Allgemeine Gleichbehandlungsgesetz (AGG) in Kraft getreten. Dieses Gesetz verpflichtet Unternehmen und Behörden, den Schutz der Beschäftigten vor Benachteiligungen aufgrund von Rasse, ethnischer Herkunft, Geschlecht, Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu gewährleisten. Insoweit gewinnt das Regelwerk sowohl auf die Personalverwaltung und Personaldatenverarbeitung als auch auf Datenschutzorganisation unmittelbaren Einfluss. Sowohl öffentliche als auch private Arbeitgeber trifft die Verpflichtung, jede Benachteiligung aus diesen Gründen zu unterlassen, zu beseitigen und zu verhindern. Dies betrifft Stellenausschreibungen, Einstellungen und Beförderungen sowie Beendigungen von Arbeitsverhältnissen und damit alle Phasen eines Arbeitsverhältnisses. Zudem ist der Schutz vor Diskriminierung in jeder betrieblich veranlassten Situation von den Arbeitgebern zu gewährleisten sowie Verstöße gegen das Diskriminierungs-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

verbot zu unterbinden und zu ahnden.

Sowohl Bewerbungsvorgänge als auch Auswahlverfahren haben sich an den Bestimmungen des Allgemeinen Gleichbehandlungsgesetzes zu orientieren (§§ 7, 11 AGG). Insbesondere sind Ausschreibungstexte so zu formulieren, dass sie weder direkt noch indirekt diskriminierend wirken. Eine Ausschreibung mit der Formulierung: "Suche Mitarbeiter in Vollzeit mit Deutsch als Muttersprache für ein junges, dynamisches Team" beinhaltet Diskriminierungsindikatoren für Nichtdeutsche, Ältere, körperlich Behinderte und Frauen, die häufig Teilzeit arbeiten. Solche Einschränkungen sind nur dann zulässig, sofern sie unverzichtbar für die Tätigkeit sind und sachlich begründet werden können (§§ 4 und 5 i. V. m. 8 bis 10 und 20 AGG). Auch die Formulierung "... Die Bewerbung von Frauen ist erwünscht", hat sich dabei an der vorhandenen Personalstruktur zu orientieren (§§ 4 und 5 AGG) und wäre z. B. bei der Besetzung einer Sekretariatsstelle wohl häufig problematisch. Von der Aufforderung zur Übersendung eines Lichtbildes ist grundsätzlich abzusehen, da diese als Indiz für eine Diskriminierung gewertet werden kann (Erkennbarkeit von Rasse, Geschlecht, Alter, evtl. Behinderung und Religion).

Bewerberfragebögen sind unter Berücksichtigung der §§ 1 und 2 Abs. 1 AGG auf die unbedingt erforderlichen Angaben zu beschränken. Auch im Vorstellungsgespräch dürfen nur Fragen gestellt werden, die für die Stelle und die Qualifikation bedeutsam sind und die Eignung des Bewerbers für die Stelle betreffen. Da nach § 15 Abs. 4 AGG im Bewerberverfahren ein Anspruch auf Schadensersatz zwei Monate nach Zugang der Ablehnung geltend gemacht werden kann, sind Bewerbungsunterlagen bzw. deren Kopien entsprechend lange in der Dienststelle aufzubewahren. Darüber hinaus sollten ausführliche Auswahlvermerke bezüglich der Bewerber angefertigt werden, um im späteren Gerichtsverfahren die Einhaltung des AGG darlegen zu können.

Darüber hinaus sind derartige Benachteiligungen nicht nur im Arbeitsleben, sondern auch im allgemeinen Zivilrechtsverkehr, also etwa bei der Vermietung von Wohnraum, der Inanspruchnahme von Gesundheitsdiensten oder beim Zugang zu Bildungseinrichtungen, grundsätzlich unzulässig.

Die Umsetzung des Allgemeinen Gleichbehandlungsgesetzes muss im Rahmen des Datenschutzrechts erfolgen. Dabei ist auch zu berücksichtigen, dass der Gesetzgeber die Merkmale, die kein Grund für Benachteiligungen sein dürfen (Rasse, Geschlecht, Alter, Religion oder Weltanschauung, sexuelle Identität), mit Ausnahme des Alters zugleich im Datenschutzrecht als besonders schutzwürdig (sensitiv) einstuft. Deshalb sind *Scoring-Verfahren*, die sich auf solche Merkmale stützen, schon nach dem Bundesdaten-

Der Senat weist darauf hin, dass bei Stellenbesetzungen in der Berliner Verwaltung außerdem die Vorschriften des Landesgleichstellungsgesetzes (LGG), insbesondere die §§ 5 ff. LGG zu beachten sind.

schutzgesetz unzulässig.

7.3.2 Reiselustige Senioren und „Geburtstagskinder“

Ein Reiseunternehmen wies die Beschäftigten an, ab sofort bei jeder Buchung die Geburtsdaten des Reisenden zu erheben. Zur Begründung teilte das Unternehmen Folgendes mit:

1. *Die Platzierung älterer Kunden oben in einem Doppeldecker-Bus solle vermieden werden.*
2. *Ältere Kunden sollen in Hotels ohne Fahrstuhl nicht in obere Etagen einquartiert werden.*
3. *Etwaige Ermäßigungen sollten konkret berechnet werden können.*
4. *Falls ein Kunde auf einer Rundreise Geburtstag habe, solle ihm gratuliert werden.*

Das Geburtsdatum gehört zu den personenbezogenen Daten, die nur unter den besonderen Voraussetzungen des § 28 BDSG erhoben werden dürfen. Danach ist eine Erhebung für die eigenen Geschäftszwecke zulässig, wenn es gemäß § 28 Abs. 1 Nr. 1 BDSG der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient oder wenn es gemäß § 28 Abs. 1 Nr. 2 BDSG zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Bezüglich der Platzierung in einem Doppeldecker-Bus bzw. der Einquartierung im Hotel reicht die entsprechende Altersstufe (z. B. über 60 Jahre alt) aus, ab der ein Reiseunternehmen erfahrungsgemäß Kunden nicht mehr im Oberdeck bzw. im Obergeschoss eines Hotels ohne Fahrstuhl unterbringen würde. Zudem sind sowohl diesseits als auch jenseits einer bestehenden Altersgrenze durchaus Abweichungen vorstellbar (so z. B. ältere Menschen, die sehr gern im Oberdeck eines Busses sitzen, oder jüngere Menschen mit einem Rückenleiden, die auch nicht im Obergeschoss eines Hotels ohne Fahrstuhl einquartiert werden wollen). Insoweit ist hier eine konkrete Nachfrage zweckmäßiger als die Kenntnis des konkreten Geburtsdatums.

Die verpflichtende Angabe des genauen Geburtsdatums ist auch nicht mit der Absicht zu rechtfertigen, den Kunden bei der Reise gratulieren zu wollen. Hier ist die Angabe optional zu gestalten mit dem entsprechenden Hinweis auf das Anliegen. Sofern ein Kunde auf eine etwaige Gratulation Wert legt, sollte ihm die Angabe seines Geburtsdatums freigestellt werden.

Anders zu beurteilen ist die Angabe des Geburtsdatums für die taggenaue Berechnung einer eventuellen Ermäßigung. Hiergegen sind grundsätzlich keine Einwände zu erheben, wenn sich die Pflichtangabe nur auf solche Personen bezieht, die sich tatsächlich in einer "Grauzone" zu den entsprechenden Altersgrenzen befinden. Nicht erforderlich scheint hingegen das Geburtsdatum einer Person, die sich erkennbar unterhalb bzw. oberhalb einer solchen Grenze befindet.

- Zum Zwecke der Altersbestimmung für das Einquartieren von Kunden in Hotels bzw. das Platzieren in Doppeldeckern ist die Angabe einer bestimmten Altersstufe (zum Beispiel über 60 etc.) zulässig, eine konkrete Nachfrage jedoch zweckmäßiger.

- Die Angabe des genauen Geburtsdatums für eine eventuelle Gratulation darf nur optional mit entsprechendem Hinweis verlangt werden

- Die verpflichtende Angabe des Geburtsdatums für die taggenaue Berechnung von Ermäßigungen ist mit entsprechendem Hinweis dann zulässig, wenn dies die Personen betrifft, die sich an einer relevanten Altersgrenze befinden und davon nicht erkennbar weit entfernt sind.

Die Frage nach dem Geburtsdatum muss bei einer Reisebuchung nur beantwortet werden, wenn davon eine altersbezogene Ermäßigung abhängt.

7.3.3 Gefährliche Hostel-Software

Ein irisches Unternehmen ist Weltmarktführer für Hostel-Software und Internet-Buchungen für Hostels. In den letzten Jahren stellte es die Hostel-Software als Download zur Verfügung. Mithilfe dieser Software werden von dem Gast folgende Daten gespeichert: Name, Adresse, E-Mail, Telefon, Aufenthaltsdaten, gastspezifische Eingaben wie etwa auffälliges Verhalten (z. B. der Hinweis, dass der Gast nicht mit Frauen in einem Zimmer übernachten sollte), gekaufte Zusatzangebote (Städtetour etc.). Das irische Unternehmen hat den deutschen Hostel-Betreibern mitgeteilt, dass die Software in Zukunft ausschließlich online auf einer Internet-Plattform zur Verfügung gestellt wird. Die deutschen Hostels befürchten, dass das irische Unternehmen die ihm durch die Nutzung der Online-Software zugänglichen Daten vermarkten wird, außerdem könnte es Einblick in die wirtschaftliche Situation der Hostels gewinnen. Das irische Unternehmen bestreitet, entsprechende Interessen zu verfolgen.

Auch wenn das irische Unternehmen die ihm zugänglichen personenbezogenen Daten der Hostel-Gäste nicht vermarkten will und in Irland ein dem deutschen Recht entsprechendes Datenschutzniveau herrscht, müssen die deutschen Hostels beachten, dass eine

Übermittlung von Gästedaten mangels Einwilligungserklärung der Betroffenen und wegen Fehlens einer Rechtsgrundlage rechtswidrig wäre. Vor der Nutzung der Online-Software müssen sie mit dem irischen Unternehmen einen Auftragsdatenverarbeitungsvertrag abschließen, der die Datensicherheit regelt und sicherstellt, dass die Daten von dem Auftragnehmer nicht für eigene Zwecke verarbeitet werden. Der Auftrag ist schriftlich zu erteilen (vgl. § 11 Abs. 2 Satz 2 BDSG i. V. m. § 126 a Bürgerliches Gesetzbuch – BGB).

Eine Online-Hostel-Software darf nur benutzt werden, wenn sichergestellt ist, dass die personenbezogenen Daten der Hostel-Gäste nicht in falsche Hände geraten.

8 Europäischer und internationaler Datenschutz

8.1 Die Europäische Union und der Datenhunger der USA

Die aufgrund der Anti-Terror-Gesetzgebung der USA seit 2004 erfolgende *Übermittlung von Flugpassagierdaten in die USA*[96] wurde vom Europäischen Gerichtshof (EuGH) für rechtswidrig befunden. Der Gerichtshof hat den zugrunde liegenden Beschluss des Rates über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den USA sowie die Entscheidung der Europäischen Kommission über die Angemessenheit des Schutzes der personenbezogenen Daten in den Passenger Name Records (PNR)[97] für nichtig erklärt[98].

Allerdings wurde mit dieser Entscheidung nur ein Scheinsieg für den Datenschutz errungen. Denn das Gericht hat sich nicht mit den vom Europäischen Parlament und der Art. 29-Datenschutzgruppe vorgebrachten inhaltlichen Einwänden auseinandergesetzt, sondern allein mit der formellen Frage, ob der EG-Vertrag i. V. m. der Europäischen Datenschutzrichtlinie 95/46/EG eine ausreichende rechtliche Basis für die Entscheidungen von Kommission und Rat enthält. Das hat der Gerichtshof verneint. Nach seiner Auffassung fallen sie in die von Art. 3 Abs. 2 Europäische Datenschutzrichtlinie genannten Bereiche der sog. Dritten Säule (Zusammenarbeit der Mitgliedstaaten in den Bereichen Justiz und Inneres). Denn die PNR-Daten würden für Zwecke der Terrorismus- und Kriminalitätsbekämpfung in die USA übermittelt. Die Europäische Datenschutzrichtlinie finde aber keine Anwendung, soweit die Verarbeitung personenbezogener Daten u. a. für Zwecke der öffentlichen Sicherheit,

[96] JB 2004, 4.7.1
[97] JB 2004, 4.7.1
[98] Urteil v. 30. Mai 2006, NJW RR, 2029

Landesverteidigung, Sicherheit des Staates und dessen Tätigkeiten im strafrechtlichen Bereich erfolgt. Daran ändere auch die Tatsache nichts, dass es private Wirtschaftsteilnehmer (Fluggesellschaften) sind, die die PNR-Daten zu gewerblichen Zwecken erhoben haben und in einen Drittstaat übermitteln.

Entsprechend der Entscheidung des EuGH galten die für nichtig erklärten rechtlichen Grundlagen übergangsweise bis Ende September weiter. Die Artikel-29-Datenschutzgruppe hatte auf die baldige Verabschiedung einer Folgevereinbarung gedrungen, bei der das Datenschutzniveau des ersten Abkommens erhalten bleiben müsse[99]. Am 6. Oktober hat die Europäische Union mit den USA ein Zwischenabkommen vereinbart, das in der sog. Dritten Säule ausgehandelt wurde. Die EU konnte sich nicht mit der Forderung durchsetzen, das Interimsabkommen inhaltsgleich wie die früheren Abkommen zu fassen. Danach durften die Zoll- und Grenzschutzbehörden in den USA die Fluggastdaten nur in Einzelfällen weitergeben. Nach dem neuen Abkommen dürfen sie routinemäßig an andere US-Sicherheitsbehörden, z. B. an die Bundespolizei FBI oder den Geheimdienst CIA, weitergegeben werden. Das neue Abkommen gilt zunächst bis Ende Juli 2007, soll aber möglichst früher durch ein endgültiges, sorgfältig ausgehandeltes ersetzt werden. Dieser Lösung wird nach wie vor gegenüber bilateralen Vereinbarungen der einzelnen EU-Mitgliedstaaten mit den USA der Vorzug gegeben.

Zwischenzeitlich wurde bekannt, dass nun auch das US-Gesundheitsministerium Flugpassagierdaten benötigt, um mit den zugleich zu erhebenden Gesundheitsdaten Reisender die Seuchenbekämpfung, insbesondere den Schutz vor der Vogelgrippe, zu verbessern. Die Art. 29-Datenschutzgruppe hat zu diesen Plänen des US-Gesundheitsministeriums Stellung genommen und festgestellt, dass sie weder mit der EU-Datenschutzrichtlinie noch den Vorschriften der Weltgesundheitsorganisation übereinstimmen[100].

Pressemeldungen zufolge[101] werden Amerika-Reisende ohne ihr Wissen bereits seit Jahren von den US-Behörden mithilfe eines Computerprogramms auf ihr terroristisches oder sonstiges kriminelles Potenzial hin überprüft. Durch die ATS (Automated Targeting System)-Analyse soll anhand bestimmter Daten der Flugpassagiere wie Herkunftsland, frühere Reisen und Art der Ticket-Bezahlung das Sicherheitsrisiko des Einzelnen für die USA nach Art eines Scoring-Verfahrens „berechnet“ werden.

---

[99] Stellungnahme 7/2006 zum Urteil des EuGH über die Übermittlung von Fluggastdaten an die Vereinigten Staaten und zur Dringlichkeit eines neuen Abkommens (WP 124) v. 27. September 2006

[100] Stellungnahme 4/2006 zu der Mitteilung eines Regelungsvorschlags des US-Department of Health and Human Services (Gesundheitsministerium der Vereinigten Staaten) zur Kontrolle übertragbarer Krankheiten und zur Erhebung von Daten über Passagiere v. 20. November 2005 (WP 121) v. 14. Juni 2006

[101] Frankfurter Rundschau v. 2. Dezember 2006, S. 6; Frankfurter Allgemeine Zeitung v. 2. Dezember 2006, S. 2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Das US-Ministerium für innere Sicherheit (Department of Homeland Security) hat inzwischen eingeräumt, dass die Transportation Security Agency während der Testphase für das Programm „Secure Flight“ vom Herbst 2004 bis Frühjahr 2005 entgegen einer anderslautenden Datenschutzerklärung auch Daten aus kommerziellen Quellen gesammelt hat[102]. Das „Secure Flight“-Programm soll dazu dienen, Passagierdaten mithilfe von Data-Mining-Techniken so zu analysieren, dass potenzielle Flugzeugentführer am Einchecken gehindert werden.

Die ständige Übermittlung von Flugpassagierdaten aus Europa an die US-Behörden erfolgt bisher nicht auf einer datenschutzgerechten Grundlage.

Mitte des Jahres war durch Veröffentlichungen der US-Medien bekannt geworden, dass US-Geheimdienste seit Jahren vertrauliche *Daten bei der Society for Worldwide Interbank Financial Telecommunication (SWIFT)* – einem Netzwerkdienstleister für internationale Finanztransaktionen – einsehen. Als Grund wurde die Bekämpfung des internationalen Terrorismus durch Aufspüren seiner Finanzaktivitäten genannt. *SWIFT* ist als Genossenschaft belgischen Rechts organisiert und 1973 von der internationalen Kreditwirtschaft gegründet worden. Sie ist ein weltweit agierender Geldüberweisungsdienst zur Übermittlung von internationalen Zahlungsanweisungen. *SWIFT* verarbeitet täglich durchschnittlich 12 Millionen Nachrichten. Im Jahr 2005 waren es insgesamt 2,5 Milliarden Nachrichten, von denen 1,6 Milliarden Europa und 467 Millionen Nord- und Südamerika betrafen. Die Organisation speichert alle Überweisungsdaten für 124 Tage in zwei Rechenzentren, von denen sich eines in Europa, das andere in den USA befindet. Aus Gründen der Datensicherheit, also um für den Ausfall oder die Zerstörung des in Europa befindlichen Rechenzentrums vorzusorgen, wird der gesamte dort befindliche Datenbestand im US-Rechenzentrum „gespiegelt“. Das gilt auch für Daten, die keinerlei Bezug zu US-amerikanischen Banken oder Kunden haben.

Das US-Finanzministerium verlangte nach den Terrorangriffen vom September 2001 von SWIFT den Zugang zu den in den USA gespeicherten Daten. Nach dem Ende September von der belgischen Datenschutzbehörde erstatteten Prüfbericht hat SWIFT sowohl gegen belgisches als auch europäisches Datenschutzrecht verstoßen. SWIFT habe bei der offensichtlich seit Jahren betriebenen Weitergabe bestimmter Kundendaten an amerikanische Behörden zu stark den amerikanischen Interessen nachgegeben und zu wenig das belgische und europäische Recht berücksichtigt.

[102] vgl. http://www.heise.de/newsletter/meldung/83510; http://www.das.gov/xlibary/asset/privacy/privacy-secure-flight-122006.pdf

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Artikel-29-Datenschutzgruppe hat zur Verarbeitung der personenbezogenen Daten durch SWIFT ebenfalls Stellung genommen[103]. Danach tragen sowohl SWIFT als auch die Banken in Europa die gemeinsame Verantwortung für die Datenverarbeitung. Hervorgehoben wurde, dass bereits bei der Entscheidung, den gesamten Datenbestand in einem US-Rechenzentrum parallel verarbeiten zu lassen, weder die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit noch die Garantien für die Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau noch die Transparenzforderungen der Europäischen Datenschutzrichtlinie beachtet worden sind. In ihrer Stellungnahme hat die Artikel-29-Datenschutzgruppe sofortige Maßnahmen zur Verbesserung der derzeitigen Situation gefordert. So sind die Rechtsverletzungen abzustellen, was notfalls mit Sank-tionen der zuständigen nationalen Aufsichtsbehörden durchgesetzt wird. Zu den Forderungen gehört auch, dass alle Finanzinstitute in der EU ihrer Verpflichtung nach Art. 10, 11 Europäische Datenschutzrichtlinie nachkommen und ihre Kunden angemessen über die Datenverarbeitung unterrichten und darüber, welche Rechte die Betroffenen haben. Die Information muss sich auch darauf erstrecken, dass die US-Behörden Zugriff auf die Daten haben können. Die Artikel-29-Datenschutzgruppe beabsichtigt, hierzu einen einheitlichen Informationstext zu erarbeiten.

Die Verarbeitung sämtlicher Daten über innereuropäische Finanztransaktionen durch SWIFT in den USA verstößt ebenso gegen europäisches Datenschutzrecht wie die unkontrollierte Weitergabe von Daten an das US-Finanzministerium. Dies gilt umso mehr, als eine unabhängige Datenschutzkontrolle in den USA nach wie vor nicht gewährleistet ist.

Trotz allem sind die EU und die USA bemüht, den *transatlantischen Dialog zum Datenschutz* fortzusetzen. So hat Ende Oktober in Brüssel der Gegenbesuch des US-Handelsministeriums stattgefunden, nachdem sich im Dezember letzten Jahres eine Delegation der Artikel-29-Datenschutzgruppe zu Gesprächen in Washington eingefunden hatte. An der von ihr gemeinsam mit der Europäischen Kommission und dem US-Handelsministerium veranstalteten Konferenz nahmen mehr als 300 Datenschutzexperten aus den USA und Europa teil. Einen Schwerpunkt bildete das mit den USA ausgehandelte *Safe-Harbor-Abkom-men*[104], dem bislang etwa 1000 Unternehmen beigetreten sind[105]. Daneben wurden Erfahrungen mit den Standardvertragsklauseln der Europäischen Kommission und den verbindlichen Unternehmensregelungen

[103] Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (WP 128) v. 22. November 2006; vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 55

[104] zuletzt JB 2002, 4.7.1

[105] vgl. http://www.export.gov/safeharbor/

als Instrumentarien für die Gewährleistung ausreichender Datenschutzgarantien ausgetauscht[106]. Leider konnte ein weiteres Problemfeld, das sich zwischenzeitlich bei den deutschen Aufsichtsbehörden in Beratungsersuchen mit der deutschen Wirtschaft herauskristallisiert hat, nicht in die Erörterungen mit der US-Seite einbezogen werden.

So wurden mehrere Konzerne durch Beschlagnahmeanordnung des amerikanischen Justizministeriums direkt verpflichtet, personenbezogene Daten über Mitarbeiter in den deutschen Niederlassungen an das US-Justizministerium zu übermitteln. Hintergrund waren die dort geführten Ermittlungen wegen Korruptionsverdachts bei verschiedenen weltweit tätigen Konzernen, die der US-Börsenaufsicht unterliegen. Diese widmet sich verstärkt dem Kampf gegen Bilanzfälschungen, die häufig durch Schmiergeldzahlungen und schwarze Kassen verursacht werden. Ähnlich wie in den oben beschriebenen Fällen befinden sich die hier betroffenen Unternehmen in einem Dilemma. Einerseits müssen sie zur Abwendung wirtschaftlicher Nachteile den Aufforderungen der USA Folge leisten. Andererseits sind sie gehalten, die datenschutzrechtlichen Vorgaben in der Europäischen Union zu beachten. Hierzu haben wir uns an das Bundesjustizministerium mit der Bitte um Prüfung gewandt, ob und in welchem Umfang nach den bestehenden Rechtshilfeübereinkommen eine Verpflichtung zur Herausgabe der vom US-Justizministerium verlangten Unterlagen besteht.

Dass nicht nur US-Regierungsstellen immer mehr personenbezogene Daten von europäischen Wirtschaftsunternehmen verlangen, sondern auch private Stellen, soll an folgendem Fall dargestellt werden, der uns zur Beratung vorgelegt wurde.

Im Rahmen eines gerichtlichen Patentverletzungsverfahrens in den USA wurde die Schering AG durch eine sog. Discovery Order des US-Gerichts verpflichtet, bestimmte E-Mails von 160 Schering-Mitarbeitern gegenüber einem US-Unternehmen offen zu legen. Die E-Mail-Konten sollten nach bestimmten Schlüsselwörtern durchsucht werden. Die offen zu legenden Informationen würden durch eine gerichtliche Schutzanordnung (Protective Order) geschützt. Die Schering AG bat uns um Mitteilung, ob das Scannen der E-Mail-Konten und das Kopieren positiv gescannter E-Mails zur Erfüllung der Discovery Order nach deutschem Datenschutzrecht zulässig oder strafbar sind (§ 206 StGB). Schließlich wurde gefragt, ob die Übermittlung der kopierten E-Mails an die Prozessvertreter von Schering in den USA sowie an die gegnerischen Anwälte zur Erfüllung der Discovery Order rechtmäßig wäre.

[106] zuletzt JB 2004, 4.7.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Mangels Freiwilligkeit der Einwilligung im Arbeitsverhältnis wurden die Maßnahmen zunächst nicht auf die Einwilligung der Mitarbeiter gestützt. Nach § 4 c Abs. 1 Satz 1 Nr. 4 BDSG ist die Datenübermittlung zulässig, sofern sie zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist. Hier stellte sich die Frage, ob die gegnerischen Anwälte und das Gericht tatsächlich die Klarnamen der betroffenen Mitarbeiter benötigen oder ob die Übermittlung der E-Mail-Inhalte mit pseudonymisierten Daten zunächst ausreicht. Wir haben empfohlen, erst dann, wenn sich nach Prüfung der Inhalte herausstellt, dass die Kenntnis der Personen „hinter den Daten“ erforderlich ist, diese zusätzlich zu offenbaren sind. Die zweistufige Verfahrensweise wurde von US-Gerichten bereits in anderen Verfahren, die die deutsche Wirtschaft betrafen, gebilligt.

Unsere Empfehlungen betrafen nur die dienstlichen E-Mails. Die privaten E-Mails, die nicht in die USA übermittelt werden sollten, waren aus dem gesamten Mail-Bestand herauszufiltern. Hierzu haben wir empfohlen, die eigenen US-Anwälte nach Deutschland zu holen, die eine entsprechende Sichtung der E-Mails durchführen könnten. Damit wäre zumindest das Problem des Drittstaatentransfers beseitigt worden.

Nach Auffassung von Schering wäre das zweistufige Verfahren wegen des finanziellen, aber auch tatsächlichen Aufwandes nicht verhältnismäßig gewesen, denn es hätte eine händische Überprüfung zumindest im Hinblick auf alle Attachments erfolgen müssen. Nach umfangreichen Beratungsgesprächen haben wir eine Vorgehensweise vorgeschlagen, der das Treuhandmodell zugrunde liegt. Ausgangspunkt der Überlegungen war der Umstand, dass die Freiwilligkeit der Mitarbeitereinwilligungen dann nicht infrage steht, wenn die Leitung des Konzerns und die mit Personalentscheidungen befassten Personen keine Kenntnis darüber erhalten, ob die betroffenen Mitarbeiter der Datenverarbeitung zugestimmt haben. Diese erhielten ein Informationsschreiben zu den geplanten Datenverarbeitungen und hatten die Wahl, eine Einverständnis- oder Verweigerungserklärung zu unterschreiben. Ihre Erklärungen wurden an einen Treuhänder geschickt, der daraufhin die Mailboxen der Zustimmenden an einen US-Dienstleister zur Durchsuchung nach bestimmten Suchbegriffen übermittelte. Der Dienstleister reiste dafür eigens nach Berlin an. Zwischen dem Treuhänder und ihm wurde eine Datenschutzvereinbarung nach den Vorgaben von § 11 BDSG geschlossen. Die Suchergebnisse wurden in Form von Ausdrucken der betreffenden E-Mails an die US-Anwälte der Schering AG geleitet, die verpflichtet waren, eventuelle private E-Mails auszusortieren und zu vernichten. Der Restbestand wurde an die gegnerischen Anwälte geschickt, die ihrerseits die Unterlagen entsprechend der gerichtlichen Protective Order nutzen mussten. Alle betroffenen Mitarbeiter hatten dem Verfahren zugestimmt.

Die Weitergabe von personenbezogenen Daten an US-Unternehmen darf selbst dann nur im Rahmen des deutschen und europäischen Datenschutzrechts erfolgen, wenn das US-amerikanische Prozessrecht dies verlangt.

8.2 Weitere Ergebnisse aus Brüssel

Die Arbeiten in der Artikel-29-Datenschutzgruppe waren vorwiegend von den Themen „*Flugpassagierdaten*“ und *SWIFT* geprägt. Daneben hat sie eine *Empfehlung zur datenschutzgerechten Ausgestaltung von firmeninternen Telefonhotlines* (sog. Whistleblowing-Systeme) beschlossen[107] und zu *Datenschutzfragen bei Filterdiensten für elektronische Post* Stellung genommen[108]. Hier wurden Entwickler von E-Mail-Software aufgefordert, datenschutzkonforme Systeme zu konzipieren. Die Artikel-29-Datenschutzgruppe hat sich auch mit einem *Musterantrag zur Anerkennung von verbindlichen Unternehmensregelungen* befasst, der im Entwurf vom International Chamber of Commerce (ICC) zur Stellungnahme vorgelegt worden war. Nach grundlegender Überarbeitung, an der auch wir uns federführend für die deutschen Aufsichtsbehörden wegen unseres Vorsitzes in der AG „Internationaler Datenverkehr“ und unserer Erfahrungen mit bereits anerkannten verbindlichen Unternehmensregelungen[109] beteiligt haben, wird der Musterantrag als Empfehlung der Datenschutzgruppe verabschiedet werden.

8.3 AG „Internationaler Datenverkehr“

Die unter unserem Vorsitz tagende AG „Internationaler Datenverkehr“ des Düsseldorfer Kreises hat sich mit Fragestellungen befasst, die sich bei der Datenverarbeitung durch weltweit agierende Konzerne ergeben und die bislang in Deutschland und wahrscheinlich auch im übrigen Europa weitestgehend ungeklärt sind. Bei der zweitägigen Sitzung mit deutschen Aufsichtsbehörden und Wirtschaftsvertretern wurden verschiedene Konstellationen diskutiert mit dem Ziel, die Aufsichtsbehörden anhand konkreter Fallgestaltungen aus der Wirtschaft über bestehende Schwierigkeiten bei der Anwendung der §§ 4 b, 4 c BDSG zu informieren. Dazu gehörte die Bestimmung der Daten exportierenden Stelle z. B. in Fällen, in denen konzernangehörige Stellen in das Konzern-Intranet oder in ein konzerneitiges Personalverwaltungs- oder sonstiges Datenveraltungssystem (z. B. SAP oder People Soft) Daten eingeben, die dort von anderen Konzerngesellschaften weltweit abgerufen werden können. Hierzu vertraten die Aufsichtsbehörden die Ansicht, dass diejenige Stelle als Datenexporteur anzusehen ist, die über die

[107] WP 117 v. 1. Februar 2006; vgl. bereits JB 2005, 4.8.2

[108] WP 118 v. 21. Februar 2006

[109] zuletzt JB 2004, 4.7.2

tatsächliche Entscheidungsbefugnis zur Datenüberittlung verfügt, z. B. durch die Entscheidung über die Zugriffsrechte anderer Konzernteile. Als Faustregel kann also gelten, dass maßgeblich ist, wer „das Tor zur Datenübermittlung ins Drittland öffnet".

Weitere Fragestellungen wurden vor dem Hintergrund des Arbeitsberichts der Ad-hoc-Arbeitsgruppe „Konerninterner Datentransfer[110]" im Hinblick darauf disutiert, ob und in welchem Umfang die innerstaatlichen Anforderungen an eine rechtmäßige Datenverarbeitung (sog. erste Stufe) auch in den Instrumentarien der sog. zweiten Stufe, insbesondere bei den Standardvertragsklauseln der Europäischen Kommission zum *Datenexport*, erfüllt sein müssen. Schließlich wurde erörtert, ob bei der Datenweitergabe von einem in Deutschland befindlichen Datenverarbeitungsdienstleister an seinen im Drittstaat befindlichen Auftraggeber die Anforderungen der §§ 4 b, 4 c BDSG gelten oder eine Datenübermittlung nicht vorliegt. All diese Fragestellungen und Antworten sollten auf der Grundlage des Informationsaustauschs mit der Wirtschaft von den Aufsichtsbehörden möglichst einheitlich behandelt werden. Es ist deshalb beabsichtigt, eine endgültige Position der Aufsichtsbehörden in Deutschland zu erarbeiten.

Durch die Veränderung im globalen Wirtschaftsverkehr stellen sich auch neue, komplexe Fragen des grenzüberschreitenden Datenschutzes, die von den deutschen Aufsichtsbehörden einheitlich beantwortet werden sollten.

9 Technik und Organisation

9.1 Datenschutzgerechter Einsatz von *RFID-Technologie*

Bereits in den zurückliegenden Jahren hatten wir über aktuelle Entwicklungen und Einsatz der RFID-Technologie ausführlich berichtet[111]. Im Berichtszeitraum haben sich sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder als auch die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich mit Fragen des datenschutzkonformen Einsatzes von RFID beschäftigt:

So hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 72. Sitzung am 26./27. Oktober 2006 in Naumburg eine Entschliessung gefasst, in der verbindliche Regelungen für den Einsatz von RFID-Technologien gefordert werden[112]. Unter anderem hat die Konferenz darauf hingewiesen, dass der Gesetzgeber die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden

[110] vgl. www.rpda.de/dezernate/datenschutz/download/arbeitsbericht-endfassung.pdf
[111] zuletzt JB 2005, 2.1
[112] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006", S. 18

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

sind, daraufhin untersuchen sollte, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind, und gefordert, in den Bereichen einzugreifen, in denen diese fehlen. Des Weiteren werden Forderungen für den Schutz der Persönlichkeitsrechte Betroffener hinsichtlich Transparenz, Kennzeichnungspflicht, des Verbots heimlicher Profilbildung, der Vermeidung unbefugter Kenntnisnahme und von Möglichkeiten zur Deaktivierung erhoben. Der Arbeitskreis Technik der Datenschutzkonferenz hat außerdem eine detaillierte Orientierungshilfe zur RFID-Technologie entwickelt[113].

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben auf ihrer Sitzung am 8./9. November 2006 in Bremen ebenfalls Empfehlungen für die datenschutzkonforme Entwicklung und Anwendung von RFID-Technologie insbesondere im Handel und im Dienstleistungssektor verabschiedet[114]. In diesem Beschluss haben die Obersten Aufsichtsbehörden insbesondere auf die neuen Herausforderungen verwiesen, vor die der Datenschutz mit der Einführung der RFID-Technologie gestellt wird. Ob nämlich auf diesen Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Sogar Informationen, die zunächst keinen Personenbezug haben mögen, weil sie z. B. allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen – z. B. mithilfe von Hintergrundsystemen – später einer konkreten Person zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie werde deshalb immer schwerer kontrollierbar sein. Den Aufsichtsbehörden erscheint es angesichts dieses Gefährdungspotenzials fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, um den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten. Sie halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen (einschließlich Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikbereich) gewahrt wird. Zusätzlich werden Handel und Dienstleistungssektor sowie die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie einzugehen.

Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten. Der Gesetzgeber sollte die besonderen Gegebenheiten

[113] http://www.datenschutz-berlin.de/to/OH-RFID.pdf

[114] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 23

beim Einsatz der RFID-Technologie daraufhin untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind und in den Bereichen greifen, in denen diese fehlen.

9.2 Behördliche Datenschutzbeauftragte

9.2.1 Gesprächskreis der behördlichen Datenschutzbeauftragten der Bezirke

Im Berichtsjahr trafen sich die bezirklichen Datenschutzbeauftragten wieder zu ihren regelmäßigen Gesprächsrunden. Zu den erörterten Fragestellungen gehörten die folgenden:

9.2.2 Weiterleitung von E-Mails

Der Vertreter eines Bezirksamts hatte darum gebeten, das Thema Weiterleitung von E-Mails bei Abwesenheit vom Dienst datenschutzrechtlich zu würdigen. In seinem Hause existiert eine IT-Vereinbarung, die die private Nutzung von E-Mail und Internet-Diensten nicht ausdrücklich ausschließt. Wenn Mitarbeiter plötzlich krank werden, kann es vorkommen, dass aus dienstlichen Gründen die eingegangenen E-Mails auch ohne Einverständnis der Dienstkraft an Vertreter oder Fachvorgesetzte weitergeleitet werden. Dabei kann es nicht vermieden werden, wenn diese neben den dienstlichen auch die privaten Briefe lesen. Um solche Fälle zu vermeiden, hat die Senatsverwaltung für Inneres im Zusammenwirken mit dem Hauptpersonalrat eine Internet-Rahmen-Dienstvereinbarung (IDV) geschaffen, in der die private Nutzung des Internets und anderer Dienste grundsätzlich nicht zulässig ist. Der Rechnungshof von Berlin kommt im Rahmen seiner bisher abgeschlossenen IT-Sicherheitsüberprüfungen sogar zu dem Ergebnis, dass unter Beachtung der IT-Sicherheitsrichtlinie eine private Nutzung von Online-Diensten auf dienstlichen Geräten nicht zulässig ist.

Wird die private Nutzung über dienstliche Hard- und Software zugelassen, muss der Dienstherr bedenken, dass er in diesem Fall als Telekommunikations- bzw. Telediensteanbieter (Provider) auftritt, und sich deshalb vorher über die technischen und organisatorischen Rahmenbedingungen und über die Rechtsfolgen im Klaren sein. Insbesondere sind das Fernmeldegeheimnis (§ 88 Telekommunikationsgesetz) und die Regelungen des Teledienstedatenschutzgesetzes zu beachten. Gibt es nur eine einheitliche E-Mail-Adresse für dienstliche und private E-Mails, so müssen aus technischen Gründen private und dienstliche E-Mails gleich behandelt werden. Bei erkennbar privaten E-Mails muss der Dienstherr also analog wie mit eingehender privater Schriftpost verfahren. Das bedeutet, dass er den betroffenen Sachbearbeiter von vornherein allgemein über das Verfahren und zusätzlich im Nachgang davon unterrichten muss, dass private E-Mails tatsächlich weitergeleitet worden sind.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Soll diese Problematik vermieden werden, ist zu empfehlen, private und dienstliche E-Mails durch einen gesonderten Account zu trennen. Durch die Einrichtung einer dienstlichen und einer zusätzlichen privaten E-Mail-Adresse kann eine Kenntnisnahme des Inhalts privater E-Mails durch Dritte weitgehend ausgeschlossen werden.

In der mit dem Hauptpersonalrat abgeschlossenen „Dienstvereinbarung über die Nutzung des Internet und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung (Internet-DV)“ vom 21.2.2002 ist festgelegt, dass „ …die private Nutzung des Internet und der anderen Dienste grundsätzlich nicht zulässig ist.“

Die E-Mail-Adressen in der Berliner Verwaltung sind somit grundsätzlich nur für dienstliche E-Mails zu verwenden. Eine Einrichtung von separaten E-Mail Adressen für private E-Mails ist daher nicht erforderlich.

9.2.3 Befristete Bestellung eines *behördlichen* Datenschutzbeauftragten

Im Zusammenhang mit der Neubestellung eines behördlichen Datenschutzbeauftragten in einer Fachhochschule gab es ein Problem, das offensichtlich auf einem Missverständnis beruhte. Der Rektor der Fachhochschule hatte in dem Bestellungsschreiben nur eine begrenzte Frist für die Amtsdauer vorgesehen und dies - ohne vorherige Absprache - dem künftigen Amtsinhaber zugeleitet. Dieser meldete sich bei uns und fragte an, ob eine solchermaßen eingeschränkte Bestellung rechtens sei.

Wir teilten dem Rektor mit, dass im Berliner Datenschutzgesetz zwar keine Ausführungen zur Dauer der Amtszeit gemacht werden, wir es jedoch für wünschenswert erachten, wenn bei diesem wichtigen Amt eine gewisse Kontinuität gewahrt würde. Aufgrund der Vielfältigkeit der Aufgaben (Beratung, Schulung, Vorabkontrolle, Verzeichnisführung) und der damit verbundenen Erarbeitung der gesetzlich verlangten Fachkunde ist es von Vorteil, wenn der interne Datenschutzbeauftragte auf unbestimmte Zeit sein Amt ausüben kann. Zudem muss der Datenschutzbeauftragte damit rechnen, dass die Frist nicht verlängert wird, wenn er sein Amt nicht hinreichend willfährig versieht. Aus diesem Grund wirkt sich die Befristung im Hinblick auf die notwendige Unabhängigkeit des Datenschutzbeauftragten negativ aus.

Vonseiten des Rektors wurde daraufhin die Bestellung korrigiert und die Dauer seiner Amtszeit auf unbestimmte Zeit festgelegt.

9.2.4 Workshop der Datenschutzbeauftragten der Amtsgerichte

Bei der ersten Sitzung im Berichtsjahr wurde die Frage behandelt, ob und wenn ja, welche Mitarbeiter einen erweiterten (vollen) Zugang zum Melderegister des Landesamts für Bürger- und Ordnungsangelegenheiten (LABO) haben (sog. LEA-Auskunft). Das automatisierte Abrufverfahren ist im Meldegesetz (§ 26 Abs. 3) bzw. in der DVO-Meldegesetz geregelt; danach haben auch die Gerichte das Recht, ein automa-

tisiertes Abrufverfahren einzurichten und befugten Mitarbeitern (sog. berechtigten Empfängern) aus bestimmten Arbeitsgebieten (z. B. Handelsregister, Nachlass- und Insolvenzverwaltung) die Möglichkeit zum Abruf zu geben. Abrufverfahren dürfen nur dann eingerichtet werden, wenn der Zugriff auf die zum Abruf bereitgehaltenen Daten ihrer Art nach für den Empfänger unter Berücksichtigung der schutzwürdigen Belange und der Aufgaben der beteiligten Stellen angemessen ist. Zusätzlich ist durch technisch-organisatorische Maßnahmen sicherzustellen, dass die Zulässigkeit im Einzelfall kontrolliert werden kann.

Die oben erwähnte "volle LEA-Auskunft" ist im Abrufverfahren nicht vorgesehen; vielmehr muss jedes Amtsgericht genau festlegen, wer im Hause welche Daten, die er für seine Aufgabenerfüllung benötigt, abrufen darf. Dabei sind strenge Maßstäbe anzulegen und einzuhalten, z. B. Grundsatz der Erhebung beim Betroffenen, Datentransparenz, Benachrichtigungspflicht, Verbot automatisierter Einzelentscheidungen.

In einem Amtsgericht beanspruchte die Präsidentin den Zugriff auf sämtliche EDV-Verzeichnisse. Auslöser war der Fall einer Mitarbeiterin, die in einer dienstlichen Angelegenheit der Präsidentin ein elektronisches Dokument in den sog. Transferbereich überspielen sollte, weil diese am Abend noch den Fall bearbeiten wollte. Die Sachbearbeiterin leitete das Dokument statt in das Transferverzeichnis aus Versehen in das sog. Homeverzeichnis, für das die Präsidentin aber keine Zugriffsberechtigung hatte. Daraufhin bat diese die IT-Stelle, ihr Zugriffsrechte auf alle Verzeichnisse des Hauses freizuschalten. Die IT-Stelle verweigerte die Ausführung mit dem Hinweis auf den Datenschutz.

Die Zulässigkeit des Zugriffs hängt von der hausinternen Regelung (Dienstvereinbarung o. Ä.) ab. Wenn die Nutzung des Bürosystems für private Zwecke zugelassen wurde, hat die Präsidentin kein Recht, auf das Homeverzeichnis zuzugreifen, da die Mitarbeiter oftmals private Dokumente hier aufbewahren. Ist die private Nutzung jedoch untersagt und handelt es sich um dienstliche Dokumente, hat die Leitung des Hauses selbstverständlich ein Einsichtsrecht.

Wie sich bei der Diskussion herausstellte, findet bei den meisten Amtsgerichten die Vereinbarung des Hauptpersonalrats Anwendung, wonach keine private Nutzung dienstlicher Computer erlaubt ist.

9.3 Schutz der *Diskretion*

Im Zuge der Neueinführung oder Neustrukturierung von Behörden, insbesondere bei der Einrichtung von Großraumbüros, erhalten wir immer wieder Hinweise, die sich auf einen mangelnden Diskretionsschutz beziehen. Obwohl Diskretion im Alltag, wie beispielsweise an Bankautomaten, mittlerweile einen selbst-

verständlichen Raum einnimmt, scheint dieses grundlegende Bedürfnis von Bürgerinnen und Bürgern bei der Planung von Beratungs- und Warteräumen keine oder nur eine sehr untergeordnete Rolle zu spielen.

So erreichten uns auch in diesem Jahr wieder Beschwerden aus den Bereichen Soziales und Finanzen, die aufgrund der Sensitivität der dort verarbeiteten Daten (Sozial- bzw. Steuergeheimnis) eine besondere Sorgfalt bei der Verarbeitung personenbezogener Daten erfordern.

Während der Kontrolle eines Jobcenters mussten wir erneut feststellen, dass der Diskretionsschutz in den Beratungs- und Wartebereichen nicht verbessert wurde. Die Zustände sind nicht nur für die Besucher des Centers, sondern auch für die Mitarbeiter ausgesprochen belastend. Verbesserungen sind aufgrund der baulichen Gegebenheiten und des hohen Besucheraufkommens häufig nicht in Sicht. Dennoch sind auch die Jobcenter verpflichtet, nach den sozialdatenschutzrechtlichen Vorschriften technische und organisatorische Maßnahmen zu treffen, um die Vertraulichkeit zu gewährleisten. Wir wiederholen an dieser Stelle unsere Forderung, hier möglichst schnell Abhilfe zu schaffen.

Es ist zu verhindern, dass Sozialdaten Unbefugten zur Kenntnis gelangen können. Bei Beratung mehrerer Hilfesuchender in einem Raum bedeutet dies, dass das Jobcenter verpflichtet ist, Einzelberatungen in einem separaten Raum anzubieten. Die Betroffenen sind durch gut sichtbare Aushänge auf diese Möglichkeit hinzuweisen. Nicht hinzunehmen ist es, wenn für die Inanspruchnahme der Einzelberatung überlange Wartezeiten in Kauf genommen werden müssen.

9.4 Einzelfragen der *Videoüberwachung*

9.4.1 Zunehmender Einsatz von Webcams im öffentlichen und öffentlich-zugänglichen Raum

Im vergangenen Jahr haben wir vermehrt Eingaben von Bürgern erhalten, die sich über die datenschutzrechtliche Zulässigkeit von Webcams informieren wollten. Der Begriff "*Webcam*" bezeichnet ursprünglich eine Webseite, auf der ein Betreiber in unterschiedlichen Intervallen aktualisierte "Live"-Bilder z. B. von öffentlichen Plätzen, Büros, Baustellen o. Ä. zeigt. Zugleich werden damit Videokameras bezeichnet, die die gemachten Aufnahmen sofort ins World Wide Web stellen können.

Die für den Betrieb notwendige Technik ist inzwischen preiswert und weltweit sehr verbreitet. Die Motive für den Betrieb einer Webcam sind unterschiedlich: Von der Hobbyausübung, Voyeurismus, Exhibitionismus und Werbung bis hin zu rein finanziellen Interessen reicht die Bandbreite einer oftmals Rund-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

um-die-Uhr-Überwachung. Webcams erlauben allerdings auch Einblicke in das Privatleben von Menschen, wie sie früher in dieser Weise nicht möglich waren.

Häufig werden Webcams auf öffentlichen Plätzen und in Einkaufspassagen als Werbemaßnahme oder "Informationsmehrwert" platziert, um auf diese Weise z. B. auf geschäftiges Treiben, Verkehrsaufkommen oder evtl. Veranstaltungen hinzuweisen. Selten werden diese Kameras von den Betreibern vordergründig zur Überwachung der Bürger genutzt, da sie häufig keine Schwenkfunktion haben und über eine stark begrenzte Auflösung (z. B. 640 x 480 Pixel) verfügen.

Dennoch sind bei der Aufnahme von Personen stets die Rechte am eigenen Bild nach dem Kunsturhebergesetz (KUG) und - bei Überwachung im öffentlich zugänglichen Raum - die Bestimmungen des § 6 b BDSG zu beachten. Datenschutzfreundlicher sind dagegen Kameraeinstellungen, die die Erkennung einzelner Personen ausschließen bzw. die keine personenbezogenen Details zulassen. Fast in Vergessenheit scheint manchmal zu geraten, dass das Kunsturhebergesetz jedem, der Bilder einer Person, die keine Person der Zeitgeschichte ist, ohne deren Einwilligung veröffentlicht, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe droht (§ 33 KUG).

Beim Einsatz von Webcams empfehlen wir Kameras mit eingeschränkten Funktionalitäten (keine Schwenk- und Zoomfunktion) und weisen auf die gesetzliche Pflicht hin, den Umstand der Beobachtung und die verantwortliche Stelle (Betreiber der Webcam) durch unübersehbare Hinweisschilder bekannt zu machen, bevor Personen den Erfassungsbereich betreten.

9.4.2 *Videoüberwachung* an Schulen

Nach dem Amoklauf eines Schülers in seiner ehemaligen Schule im nordrhein-westfälischen Emsdetten im November 2006 entbrannte erneut die Diskussion um mehr Sicherheit an Schulen. In diesem Zusammenhang wurde auch mehrfach die Videoüberwachung als mögliche Schutzmaßnahme für Schüler und Lehrer genannt.

Häufig werden die Videokameras einen solchen Schutz nicht gewährleisten können. Schon an der Eignung von Videokameras fehlt es: Wer eine Waffe versteckt in die Schule bringen will, wird von einer Kamera nicht erkannt. Wenn der Waffenbesitz an Schulen hierzulande nicht anders kontrolliert werden kann, dann muss über den Einsatz von Metalldetektoren nachgedacht werden, wie sie in den USA bereits üblich sind.

Grundsätzlich muss vor Durchführung einer solchen Maßnahme immer geprüft werden, ob die Überwachung verhältnismäßig und geeignet ist, die poten-

Der Senat teilt die Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Videoüberwachung an Schulen kann nur eine Ergänzung eines gesamtheitlichen Lösungskonzepts sein und nur in Betracht kommen, wenn und wo eine zeitnahe Reaktion eines Verantwortlichen gewährleistet werden kann.

zielle Gefahr einzudämmen.

Andererseits kann es zulässig sein, beispielsweise in unübersichtlichen Eingangsbereichen von Schulen eine Videoüberwachung zu installieren, um Schüler wie Lehrer vor Straftaten zu schützen. Die Videokamera als "Zucht- und Erziehungsmittel" dürfte jedoch allein wegen ihrer Ungeeignetheit und ihrer Unvereinbarkeit mit den Zielen des Berliner Schulgesetzes unzulässig sein. Die Installation einer Videokamera auf dem Schulhof zur Überwachung der Schüler in der Pause käme einer pädagogischen Bankrotterklärung gleich.

Videoüberwachung in einer Schule kann - wie in anderen öffentlichen und öffentlich zugänglichen Bereichen auch - ausschließlich zur späteren Rekonstruktion und Aufklärung einer begangenen Straftat dienen. Sie führt jedoch in keiner Weise zum erhofften Ziel der Vereitelung einer Tat.

Ein zur Selbsttötung entschlossener Schüler wird sich ebenso wenig wie ein Terrorist von einer Videokamera abschrecken lassen. Präventive Videoüberwachung ist daher kein geeignetes Mittel, um einen Amoklauf in einer Schule zu verhindern.

9.5 Gefahren für Notebooks

Haben Sie schon mal in Ihre Tasche gegriffen und verzweifelt festgestellt, dass Ihr mobiles Gerät nicht mehr da war? Nein? Dann haben Sie Glück gehabt oder waren vorsichtig! Außerdem sind elektronische Geräte, die unbeaufsichtigt liegen gelassen werden, schnell gestohlen. Die meisten Computer-Diebstähle finden am Arbeitsplatz statt. Weitere Orte, an denen moderne, hochwertige Elektrotechnik abhandenkommt, sind zum Beispiel:

- Verkehrsmittel und damit verbundene Orte (Autos, öffentliche Verkehrsmittel, Raststätten, Flughäfen, Bahnhöfe ...),
- Konferenzen und Messen,
- Bars.

Die Möglichkeiten dieser Geräte werden immer vielfältiger und reichen über den ursprünglichen Verwendungszweck weit hinaus. Das Risiko des Verlustes berücksichtigen die wenigsten und es wird immer noch viel zu wenig für den Schutz der auf diesen Geräten vorhandenen Daten getan, obwohl es ausreichend Schutzsoftware, z. B. zur Gewährleistung der Vertraulichkeit der gespeicherten Daten, am Markt gibt. Der Einsatz z. B. von Notebooks nimmt immer mehr zu, da Arbeiten nicht mehr ausschließlich im Büro, sondern unterwegs oder am heimischen Arbeitsplatz erfolgen. In diesem Zusammenhang wird auch oft vom sog. Information Worker gesprochen.

Gerade das Gedränge an hektischen Orten, wie z. B. auf einem Flughafen, wird von Kriminellen zum Dieb-

stahl dieser Geräte genutzt. Die auf den Geräten gespeicherten Daten müssen nicht das Ziel für die Übergriffe sein, aber für den Betroffenen kann der Diebstahl existenzbedrohende Ausmaße haben. So bekommt z. B. die Konkurrenz kostengünstig die gewünschten Informationen zu Projekten, Partnern oder Kunden.

Doch es muss nicht unbedingt ein Diebstahl sein, oft genug werden die technischen Geräte auf Flughäfen, Bahnhöfen oder im Taxi einfach liegen gelassen. Nicht abgeholte Geräte werden dann nach einer entsprechenden Zeit - mit gesäuberter Festplatte – versteigert. Die Daten lassen sich jedoch häufig mit speziellen Tools wiederherstellen.

Auch das Wegbringen oder Abholen der Kinder in den Kindergarten, der kurze Halt an einer Raststätte oder die Bezahlung in der Tankstelle gefährden öfters die mitgeführten technischen Geräte, da für diese kurzen Momente das Fahrzeug unverschlossen und möglicherweise mit steckendem Autoschlüssel verlassen wird.

Die Sicherheit ist ein kritisches Thema, dessen sich die Gerätehersteller angenommen haben. Folgende Komponenten sind häufig schon Teil des Lieferumfangs:

- Zugriffskontrolle mittels:
  - Embedded-Security-Konzept, wie z. B. der Abfrage von Passwörtern vor dem Start des Betriebssystems oder der Daten auf der Festplatte,
  - biometrischer Anmeldung z. B. per Fingerprint,
  - Smartcard-Leser für den individuellen Zugriff auf Festplattenbereiche und Dateien,
  - Authentifizierung durch Zugriffstoken, oft auf USB-Speichermedien;
- Einsatz eines sog. TPM-Sicherheitschips, der z. B. die Festplatte mithilfe eines verschlüsselten Passwortes schützen kann;
- integrierter Diebstahlschutz;
- Schutz der Schnittstellen des Notebooks wie z. B. der USB-Schnittstelle durch spezielle Software oder Deaktivierung im BIOS, das dann natürlich durch ein Passwort gegen unbefugten Zugriff geschützt werden muss;
- Schutz vor schadhaftem Code;
- Schutz vor unberechtigtem Mitlesen des Monitorinhaltes durch entsprechendes Verhalten oder Anbringen spezieller Filter.

Natürlich ist die Softwareindustrie auch nicht untätig auf diesem Sektor. So gibt es z. B. Möglichkeiten zur Löschung von Datenbeständen oder zur Verfolgung des Gerätes über das Internet bzw. durch sog. „heimtelefonierende“ Notebooks.

Damit keine sensitiven Daten Unberechtigten zur

Kenntnis gelangen, kann ausschließlich der Einsatz der Kryptografie hier angemessen schützen. Ob die Verschlüsselung der kompletten Festplatte oder einzelner Bereiche durch einen bekannten offengelegten Algorithmus erfolgt, kann nur nach Abwägung der Risiken für die gespeicherten Daten entschieden werden.

9.6 Schadhafter Code

Der Internetbrowser startet mit einer unbekannten Seite zu unglaublich günstigen Krediten oder eindeutig zweideutigen Sexangeboten. Die Firewall meldet blockierte Ports und der Router (Vermittlungsrechner, der mehrere Rechnernetze - z. B. das Internet – miteinander verbindet) blinkt hektisch. Der Virenscanner schaltet sich selbstständig unmittelbar nach dem Systemstart aus oder lässt keine Aktualisierungsupdates mehr zu. Dies alles können mögliche Anzeichen einer Infektion mit schadhaften Code wie z. B. einem Computerwurm sein. Die Sicherheit des Computers wird von vielen Seiten bedroht.

Immer wieder werden kritische Sicherheitslücken bei Softwareprodukten bekannt. Die Hersteller sind dann bemüht, diese Schlupflöcher zu stopfen, der Computer bleibt jedoch zumindest bis zur Veröffentlichung dann herausgegebener Patchs angreifbar. Zudem werden im Internet spezielle Werkzeugkästen angeboten, die gezielt diese Schwachstellen ausnutzen und z. B. das Platzieren eines Trojaners auf einem fremden Computer ermöglichen.

Doch was ist zu tun, wenn sich der Computer verdächtig verhält? Am besten ist es, wenn von einem garantiert sauberen, nicht infizierten System gebootet werden kann. Hierzu ist entweder eine originale Boot-CD (z. B. MS Windows-CD) notwendig, von der ein Virenscanner mit aktuellen Virusdefinitionen bzw. –updates gestartet werden kann, um die Festplatte(n) zu überprüfen, oder es wird z. B. eine "Knoppicillin-CD" (meist kostenlose Beilage in Computermagazinen) genutzt, auf welcher sich Virenscanner- und Festplattentools befinden. Beides muss jedoch nicht zum Erfolg führen, da zuerst ein schadhafter Code auftritt und die Virenscannerhersteller im Anschluss (teilweise um ein bis zwei Wochen verzögert) ein entsprechendes Update herausgeben. Weitere Hinweise zu Computerviren und anderen Softwareangriffen können unter anderem dem von uns herausgegebenen "Ratgeber zum Datenschutz 4" entnommen werden.

Natürlich kann auch bei einer Diagnose per Hand auf Verdächtigkeiten überprüft werden. Erste Anlaufstelle für Kontrollen sollten die Run-Keys in der Windows-Registry sein, da sich hier sehr gerne Programme eintragen, die automatisch vom System gestartet werden. Weitere Möglichkeiten sind zum einen die Kontrolle der laufenden Prozesse und zum anderen die Kontrolle

der Netzaktivitäten. Natürlich kann hier keine vollständige Aufzählung erfolgen. Doch Tools[115] zur Unterstützung sind im Internet reichlich vorhanden.

Die Reinigung eines Systems erfolgt meist automatisiert durch die Reinigungsroutine z. B. der Antivirensoftware. Hierbei muss jedoch immer berücksichtigt werden, dass ein Trojaner gelöscht wurde, die inzwischen nachgeladenen Programme oder Hintertüren jedoch übersehen wurden und als Sicherheitslücke im System verbleiben. Diese weiteren Hinterlassenschaften können evtl. wie beschrieben aufgefunden werden, empfehlen kann man jedoch nur eine Radikalkur, wobei das System komplett neu aufgesetzt wird. Mögliche Konsequenzen für Anwender, die davor zurückschrecken, können sehr vielschichtig sein. Ein Programmabsturz oder Merkwürdigkeiten bei der Ausführung von Programmen führen zu Verunsicherungen und zwingen den Computer zu einem Zeitpunkt neu aufzusetzen, an dem man es am wenigsten gebrauchen kann.

Über folgende Mindestanforderungen bzw. –ausstattungen sollten heutige Computer verfügen, damit ein Schutz vor schadhaftem Code gewährleistet ist:

- Installation und Aktivierung eines Virenschutzprogramms sowie regelmäßige Einspielung der Aktualisierungen (wie bereits oben erwähnt),
- regelmäßige Aktualisierung des Betriebssystems bzw. installierter Software (z. B. des Internetbrowsers),
- Installation einer Firewall, die diverse Zugriffe von außen sperrt,
- Nutzung alternativer Browser, da die bekannteren oft angegriffen werden,
- Einrichtung eines Nutzers mit eingeschränkten Rechten für die Verbindung mit dem Internet, damit sich unter diesem Account z. B. keine Programme installieren lassen,
- Anlage regelmäßiger Backups der Daten auf externen Datenträgern (z. B. wiederbeschreibbare CD),
- Löschung unbekannter E-Mails und
- aufmerksames und wachsames Verhalten.

Doch auch all diese Schutzvorkehrungen können mithilfe von Rootkit-Techniken unterlaufen werden. Rootkits bestehen aus einem Satz von Programmen und Code, der dauerhaft ist und kaum entdeckt werden kann. Somit können Dateien, Verzeichnisse, Registry-Einträge usw. versteckt werden. Aber auch hier gibt es bereits erste Programme, die erfolgreich Rootkits aufspüren können.

Auch für die immer häufiger auftretenden *Spyware*-

[115] z. B. von Sysinternals: http://www.microsoft.com/technet/sysinternals/default.mspx

programme (Spionageprogramme) gibt es spezielle Suchprogramme. Hierbei findet eine Erkennung von Programmen statt, deren Ziel die verdeckte Überwachung von Aktivitäten am Computer zur Ausspähung personenbezogener Daten (Kenn- und Passwörter, Kontonummern usw.) ist.

Seit 2005 sind die Begriffe *Phishing* und Pharming bei Internet-Nutzern bekannt. Beim Phishing wird meist eine Flut von Spam-E-Mails verschickt, wobei die Nachrichten so formuliert werden, als ob z. B. die Hausbank private Informationen (z. B. Einzelheiten zu Bankkonten) vom Nutzer abfragt. Hierzu wird der Anwender auf eine gefälschte Homepage per Link in der Mail geschleust. Diese Informationen werden dann selbst ausgenutzt oder weiterverkauft. Beim Pharming wird die IP-Adresse einer Homepage durch die eigene IP-Adresse eines Fälschers ersetzt. Der Nutzer bekommt von dieser Umleitung nichts mit.

Die Sicherheit eines Computers ist von vielen Seiten bedroht. Zunächst gibt es die Bedrohung, bevor ein Gegenmittel entwickelt wird (z. B. erst der Computervirus, dann die Aktualisierung der Antivirensoftware zum Auffinden und Beseitigen). Sorgfältiger, risikobewusster Umgang mit dem Medium (nicht jeder Anhang einer E-Mail muss betrachtet werden) und der sinnvolle Einsatz der diversen Schutzsoftware beim Einsatz moderner technischer Geräte können helfen.

10 Telekommunikation und Medien

10.1 Telekommunikationsdienste

10.1.1 Europäische Union: Novellierung der Telekommunikations-Datenschutzrichtlinie

Die Europäische Kommission bereitet gegenwärtig die Überarbeitung des Regulierungsrahmens für elektronische Kommunikationsnetze und -dienste vor[116]. Ein hierzu veröffentlichtes Arbeitspapier[117] sieht u. a. die Einführung von Verpflichtungen der Anbieter vor, Sicherheitsmaßnahmen zu treffen, sowie Befugnisse für die zuständigen Regulierungsbehörden, deren technische Umsetzung zu überwachen[118]. Derartige Befugnisse und Verpflichtungen sind gegenwärtig nicht in allen Mitgliedstaaten vorhanden, während das deutsche Telekommunikationsrecht dies bereits jetzt vorsieht (§ 109 des Telekommunikationsgesetzes – TKG).

---

[116] vgl. die Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste v. 29. Juni 2006, KOM(2006) 334 endg.

[117] SEC(2006) 816 v. 28 Juni 2006; http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf

[118] SEC(2006) 816, S. 28 unter 7.1

Darüber hinaus sollen Netzbetreiber und Internet Service Provider verpflichtet werden, ihre Kunden über Sicherheitsvorfälle zu informieren, die zum Verlust, zur Veränderung oder zur Zerstörung von oder zum unbefugten Zugriff auf ihre personenbezogenen Daten geführt haben. Sie sollen ebenfalls verpflichtet sein, die nationale Regulierungsbehörde über solche Vorfälle zu informieren[119]. Entsprechende Meldepflichten sind bereits in einzelnen US-Bundesstaaten (z. B. Kalifornien) geltendes Recht und haben zur Aufdeckung erheblicher Sicherheitsmängel bei amerikanischen Unternehmen in einer ganzen Reihe von Fällen geführt. Zugleich hat die damit verbundene Publizität das öffentliche Datenschutzbewusstsein in den USA geschärft und eine Diskussion über mögliche Maßnahmen des Gesetzgebers zur Verbesserung des Datenschutzes ausgelöst.

Die Artikel-29-Datenschutzgruppe hat zur Überprüfung des Rechtsrahmens im Hinblick auf die Datenschutzrichtlinie für elektronische Kommunikation Stellung genommen[120]. Sie hat insbesondere den Vorschlag zur Meldung von Sicherheitsverstößen durch Netzbetreiber und Diensteanbieter an Regulierungsbehörden und betroffene Kunden begrüßt, zugleich aber angemerkt, dass es hinsichtlich der geplanten Meldung an die Regulierungsbehörde an wirksamen Sanktionen fehlt und dass derartige Meldepflichten auch für „Datenmakler“, Banken und andere Anbieter von Online-Diensten in Betracht gezogen werden sollten. Darüber hinaus hält die Arbeitsgruppe bei schwerwiegenden Verstößen gegen die Sicherheit eine Information nur der unmittelbar betroffenen Kunden nicht für ausreichend und regt an, dass in diesen Fällen alle Kunden eines Diensteanbieters informiert werden sollen.

Die Arbeitsgruppe hat darüber hinaus darauf hingewiesen, dass gegenwärtig in einigen Mitgliedstaaten die Datenschutzbehörden nur über eingeschränkte Ermittlungsbefugnisse zum Nachweis eines Verstoßes gegen die Regelungen der Richtlinie verfügen, und entsprechende Verbesserungen gefordert.

10.1.2 Richtlinie zur *Vorratsdatenspeicherung* beschlossen

Der 15. März 2006 dürfte als ein schwarzer Tag in die Geschichte des Datenschutzes eingehen: An diesem Tag wurde die Richtlinie der Europäischen Union zur Vorratsdatenspeicherung beschlossen[121]. Damit haben

[119] SEC(2006) 816, S. 29 f. unter 7.2

[120] Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation (WP 126) v. 26. September 2006; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_de.pdf

[121] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates v. 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer

sich die Befürchtungen, über die wir bereits in unserem Jahresbericht 2005[122] berichtet hatten, bewahrheitet. Gemäß der Richtlinie sind zukünftig bestimmte Datenkategorien auf Vorrat zu speichern, d. h. unabhängig davon, ob sie für eigene Zwecke der Anbieter von Telekommunikationsdienstleistungen nach Ende der Verbindung – z. B. zur Abrechnung mit dem Teilnehmer – noch erforderlich sind. Die Richtlinie enthält hierzu einen umfangreichen Katalog, der nicht nur Verbindungen im Telefonfestnetz und im Mobilfunk betrifft, sondern auch Daten zum Internetzugang, zur Internet-Telefonie und zur Internet-E-Mail. Dabei handelt es sich im Einzelnen um:

Für Telefonfestnetz und Mobilfunk:

- die Rufnummer des anrufenden Anschlusses sowie den Namen und die Anschrift des Teilnehmers oder registrierten Nutzers,
- die angewählte(n) Rufnummer(n) (d. h. die Rufnummer(n) des angerufenen Anschlusses und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird) sowie Namen und Anschriften der Teilnehmer oder registrierten Benutzer,
- Datum und Uhrzeit des Beginns und des Endes eines Telekommunikationsvorgangs,
- den in Anspruch genommenen Telefondienst,
- zusätzlich für Mobilfunkverbindungen: die internationale Mobilteilnehmerkennung (IMSI) und die internationale Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses sowie im Falle vorausbezahlter anonymer Dienste Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standortes (Cell-ID), an dem der Dienst aktiviert wurde.

Bei Internet-Zugang, Internet-E-Mail und Internet-Telefonie:

- die zugewiesene(n) Benutzerkennung(en),
- die Benutzerkennung und die Rufnummer, die einer jeden Nachricht im öffentlichen Telefonnetz zugewiesen werden,
- den Namen und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll-Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war,
- die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie,
- die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennungen des vorgesehenen Empfängers einer Nachricht,

---

Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG; ABl. EU L 105/54

[122] vgl. dort unter 5.1

- Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers,
- Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone,
- den in Anspruch genommenen Internetdienst,
- die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
- den digitalen Teilnehmeranschluss (DSL) oder einen anderen Endpunkt des Urhebers des Kommunikationsvorgangs.

Im Falle der Nutzung mobiler Geräte sollen weiterhin zur Bestimmung des Standorts dieser Geräte folgende Daten gespeichert werden:

- die *Standortkennung* (Cell-ID) bei Beginn der Verbindung,
- Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt[123].

Dies gilt allerdings nur, soweit die Daten von Anbietern öffentlich zugänglicher elektronischer Telekommunikationsdienste oder Betreibern öffentlich zugänglicher elektronischer Kommunikationsnetze ohnehin im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden[124]. Soweit derartige Daten nicht von diesen Anbietern erzeugt oder verarbeitet werden, besteht auch keine Pflicht zur Vorratsdatenspeicherung[125]. Die Einführung zusätzlicher Erhebungsbefugnisse bzw. -verpflichtungen kann also nicht auf diese Richtlinie gestützt werden. Auch darauf wird im Rahmen der Umsetzung in nationales Recht zu achten sein.

Hinsichtlich der Speicherungsdauer wird den Mitgliedstaaten ein Spielraum eröffnet. Sie können vorsehen, dass die entsprechenden Daten für einen Zeitraum von mindestens sechs Monaten, aber höchsten zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

Zweck der Speicherung ist ausweislich der in der Richtlinie selbst enthaltenen Definition sicherzustellen, „... dass die Daten zum Zwecke der Ermittlung,

[123] Artikel 5 Abs. 1 Richtlinie 2006/24/EG
[124] Artikel 1 Abs. 1, 3 Abs. 1 Richtlinie 2006/24/EG
[125] Erwägungsgrund 23 Richtlinie 2006/24/EG

Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen[126]." Die Richtlinie muss bis zum 15. September 2007 in nationales Recht umgesetzt werden. In Bezug auf Internetzugang, Internet-Telefonie und Internet-E-Mail kann jeder Mitgliedstaat die Anwendung der Richtlinie bis zum 15. März 2009 aufschieben. Deutschland hat eine Protokollerklärung zu der Richtlinie abgegeben, in der es sich das Recht vorbehält, die Anwendung der Richtlinie entsprechend zurückzustellen.

Die Umsetzung dieser Richtlinie in deutsches Recht wird mit weitreichenden Folgen für den Schutz der Privatsphäre der Nutzer von Telekommunikationsdiensten und des Internets verbunden sein. Die Artikel-29-Datenschutzgruppe hat zu Recht festgestellt, dass die Entscheidung, wonach zur Bekämpfung schwerer Straftaten Daten auf Vorrat gespeichert werden dürfen, ein absolutes Novum mit historischem Ausmaß darstellt[127]. Dies betrifft vor allem die Internetnutzung und die Nutzung von E-Mail-Diensten, bei denen im Gegensatz zu herkömmlichen Telekommunikationsdiensten bisher überhaupt keine oder nur sehr wenige personenbezogene Daten der Nutzer dauerhaft gespeichert werden. Damit wird eine Infrastruktur geschaffen, mit der nicht nur Sender und Empfänger jeder einzelnen E-Mail identifiziert werden können. Es wird darüber hinaus zukünftig auch möglich sein, jeden einzelnen Aufruf einer beliebigen Seite im Internet einem Nutzer zuzuordnen, wenn die aufgrund der Richtlinie gespeicherten Daten mit Logdateien der entsprechenden Anbieter zusammengeführt werden.

Dies ist insbesondere im Hinblick darauf bedenklich, dass im Zuge der Konvergenz von Internet- und Telekommunikationsdiensten sowie des Rundfunks immer mehr Medienangebote in das Internet verlagert werden. Die so entstehenden Datenbestände geben also nicht nur Auskunft über die Individualkommunikation, sondern erlauben es potenziell auch nachzuvollziehen, wer z. B. welche Artikel in elektronischen Zeitungen oder Video- bzw. Fernsehsendungen, die über das Internet verbreitet werden, angesehen hat. Derartige Nutzungen würden zwar über den Anwendungsbereich der Richtlinie hinausgehen, die Erfahrung lehrt jedoch, dass einmal vorhandene Daten auf lange Sicht Begehrlichkeiten auch bei weiteren Interessengruppen wecken werden. Ein erstes Beispiel hierfür bildet das Vorhaben, den Inhabern von Urheberrechten zur Verfolgung von Urheberrechtsverletzungen in Tauschbörsen Verkehrsdaten zur Verfügung zu stel-

[126] Artikel 1 Abs. 1 Richtlinie 2006/24/EG

[127] vgl. Stellungnahme 3/2006 zur Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (WP 119) v. 25. März 2006, S. 2; vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006", S. 52

len[128]. Weitere werden folgen.

Damit hat auch eine datenschutzfreundliche Entscheidung des Bundesgerichtshofs vom November 2006 wohl bald nur noch symbolische Bedeutung: Nachdem das Amtsgericht wie auch das Landgericht Darmstadt die bisherige Praxis von T-Online, auch bei Internet-Pauschaltarifen die IP-Adressen ihrer Nutzer zu speichern, obwohl diese für die Abrechnung nicht erforderlich waren, für rechtswidrig erklärt und auch eine Revision nicht zugelassen hatte, wollte T-Online beim BGH eine Zulassung der Revision durch eine Beschwerde erreichen, die der Bundesgerichtshof jedoch abgelehnt hat[129].

Sobald die Richtlinie in deutsches Recht umgesetzt wird (ein entsprechender Entwurf des Bundesjustizministeriums liegt bereits vor), wird das Bundesverfassungsgericht zu überprüfen haben, inwieweit ein solches Gesetz gegen das deutsche Grundgesetz verstößt. Es kann als sicher gelten, dass Betroffene zu diesem Zweck das Bundesverfassungsgericht anrufen werden. An der Vereinbarkeit mit deutschem Verfassungsrecht und mit europäischem Recht bestehen erhebliche Zweifel: So kommt ein Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages zu dem Schluss, dass erhebliche Bedenken bestehen, ob die Richtlinie in der beschlossenen Form überhaupt mit dem Europarecht vereinbar ist. Dies betrifft zum einen die Wahl der Rechtsgrundlage, zum anderen aber auch die Vereinbarkeit mit den im Gemeinschaftsrecht anerkannten Grundrechten[130]. Zwei Mitgliedstaaten der Europäischen Union haben bereits den Europäischen Gerichtshof angerufen, um die Richtlinie überprüfen zu lassen.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat sich deshalb öffentlich für ein Moratorium eingesetzt, das einen Aufschub der Umsetzung der Vorratsdaten-Richtlinie bis zur Entscheidung des Europäischen Gerichtshofs zur Folge hätte. Deutschland gehört sonst nicht zu den Vorreitern bei der Umsetzung von EU-Richtlinien; in diesem Fall gibt es gute Gründe, die Richtlinie erst dann umzusetzen, wenn jedenfalls ihre Konformität mit dem Europarecht gerichtlich überprüft worden ist. Ob die Richtlinie auch ohne Verstoß gegen das Grundgesetz in deutsches Recht übernommen werden kann, wird jedenfalls davon abhängen, ob der Gesetzgeber die Spielräume, die das Gemeinschaftsrecht eröffnet, verfassungskonform ausschöpft.

Dass die Richtlinie die Mitgliedstaaten ausnahmslos

---

[128] vgl. 10.1.3

[129] Beschluss v. 26. Oktober 2006 – III ZR 40/06

[130] vgl. Wissenschaftliche Dienste des Deutschen Bundestages: Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht, Ausarbeitung WD 3 – 282/06 v. 3. August 2006, S. 9

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

zur Vorratsdatenspeicherung verpflichtet, wird sich auch in Bereichen auswirken, in denen die Kommunikationsbeziehungen bisher besonders geschützt sind: So kommt ein Gutachten des Wissenschaftlichen Dienstes des Schleswig-Holsteinischen Landtags vom Februar 2006 zu dem Ergebnis, dass „... angesichts der zwingenden Vorratsdatenspeicherung ... eine Beeinträchtigung der Abgeordnetenrechte des Schleswig-Holsteinischen Landtags ... denkbar [erscheint]. Bereits die automatische Datenspeicherung vermag eine jederzeit realisierbare Beeinträchtigungsgefahr für die Vertraulichkeit der Kommunikation zwischen Abgeordneten und Bürgern/-innen hervorzurufen“[131].

Die Artikel-29-Datenschutzgruppe hat in einer Stellungnahme vom März 2006 die Mitgliedstaaten aufgefordert, angemessene und besondere Schutzvorkehrungen einzuführen, damit die Richtlinienbestimmungen einheitlich umgesetzt und die Anforderungen gemäß Artikel 8 der Europäischen Menschenrechtskonvention erfüllt werden. Dazu gehört eine strikte Zweckbindung der Verwendung der Daten auf die Übermittlung, Feststellung und Verfolgung schwerer Straftaten und ein begrenzter Zugriff eigens benannter Strafverfolgungsbehörden auf diese Daten, der grundsätzlich in jedem Einzelfall von einer Justizbehörde ordnungsgemäß genehmigt werden muss. Die Arbeitsgruppe fordert auch, dass im Rahmen der Datensparsamkeit so wenig Daten wie möglich auf Vorrat gespeichert werden sollen und dass diese nicht mittels Data Mining, etwa zum Zwecke der Feststellung des Reise- und Kommunikationsverhaltens von Personen, die von den Strafverfolgungsbehörden nicht zum Kreis der Verdächtigen gezählt werden, ausgewertet werden dürfen.

Anbietern öffentlicher elektronischer Kommunikationsdienste oder Betreibern öffentlicher Kommunikationsnetze soll es verboten werden, die gemäß der Richtlinie auf Vorrat gespeicherten Daten für andere – insbesondere ihre eigenen – Zwecke zu verarbeiten und zu nutzen. Die Daten sollen in Systemen gespeichert werden, die logisch von denen getrennt sind, die die Anbieter für ihre geschäftlichen Zwecke verwenden. Schließlich hält die Arbeitsgruppe im Bereich der Sicherheitsmaßnahmen die Schaffung von Mindeststandards für erforderlich, die genau regeln, welche technischen und organisatorischen Sicherheitsvorkehrungen die Anbieter treffen müssen[132].

Die Umsetzung der EU-Vorratsdatenrichtlinie in deutsches Recht sollte so lange aufgeschoben werden, bis der Europäische Gerichtshof über die Vereinbarkeit

---

131 vgl. http://www.sh-landtag.de/infothek/wahl16/umdrucke/0600/umdruck-16-0620.pdf, S. 2 f.

132 vgl. Stellungnahme 3/2006 zur Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (WP 119) v. 25. März 2006; vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 52

der Richtlinie mit dem Gemeinschaftsrecht, insbesondere mit den Grundrechten der Unionsbürger, entschieden hat. Der Senat sollte sich auf Bundesebene für ein solches Moratorium einsetzen.

10.1.3 Drohende Aushöhlung des *Fernmeldegeheimnisses* im *Urheberrecht*

Im Januar 2006 wurde ein Referentenentwurf für ein „Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ aus dem Bundesministerium der Justiz öffentlich bekannt, mit dem eine Europäische Richtlinie[133] umgesetzt und neue Instrumente zum Schutz von Urheberrechten und anderen gewerblichen Schutzrechten eingeführt werden sollen.

Nach den dort vorgeschlagenen Regelungen sollen zukünftig Inhabern von Urheberrechten in bestimmten Fällen auch Auskunftsansprüche gegenüber unbeteiligten Dritten zustehen, die selbst keine Verletzung von Urheberrechten begangen haben: So ist vorgesehen, dass Internet-Provider auch über durch das Fernmeldegeheimnis geschützte Daten ihrer Nutzerinnen und Nutzer Auskunft erteilen sollen, damit Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder von Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vor dieser Entwicklung ausdrücklich gewarnt[134]. Sie haben insbesondere darauf hingewiesen, dass damit erstmals das Fernmeldegeheimnis auch zugunsten privater wirtschaftlicher Interessen eingeschränkt werden soll, und ihrer Befürchtung Ausdruck gegeben, dass damit ähnliche Begehrlichkeiten weiterer Interessengruppen geweckt werden würden. Die Datenschutzbeauftragten haben auch auf den Zusammenhang mit den beabsichtigten Regelungen zur zwangsweisen Vorratsdatenspeicherung von Verkehrs- und Bestandsdaten hingewiesen. Es wäre völlig inakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Sie haben angeregt, dass Musik- und Filmindustrie selbst dafür Sorge tragen sollten, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Darüber hinaus ist festzustellen, dass die dem Referentenentwurf zugrunde liegende Richtlinie – anders als teilweise z. B. in der Presse dargestellt – den Mit-

[133] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates v. 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. EU L 195/16

[134] vgl. Entschließung der 71. Konferenz v. 16./17. März 2006 in Magdeburg: „Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 10

gliedstaaten keineswegs zwingend vorschreibt, zur Erfüllung des in Artikel 8 der Richtlinie vorgesehenen Auskunftsanspruchs auch die Mitteilung von Verkehrsdaten und damit einen Eingriff in das Fernmeldegeheimnis vorzusehen. Vielmehr ist im Gegenteil der in dem Referentenentwurf vorgesehene Auskunftsanspruch gegen Internet-Provider selbst als europarechtswidrig anzusehen: Artikel 15 Abs. 1 der Europäischen Datenschutzrichtlinie für elektronische Kommunikation[135] legt fest, dass eine Verarbeitung von Verkehrsdaten über die in der Richtlinie enthaltenen Erlaubnistatbestände hinaus nur zulässig ist, soweit dies „... für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“ Die vorgesehene Einführung von Auskunftspflichten der Internet-Provider gegenüber privaten Dritten zur Verfolgung von deren Interessen genügt diesen Anforderungen nicht. Rechtswidrig wäre jedenfalls die Einbeziehung von Daten, die nur aufgrund der zu erwartenden Umsetzung der Richtlinie zur Vorratsdatenspeicherung bei den Anbietern gespeichert werden müssen. Hierzu enthält der Entwurf keine Ausnahmen.

Von der Einführung eines Auskunftsanspruchs für Inhaber von Urheberrechten in Bezug auf die durch das Fernmeldegeheimnis geschützten Verkehrsdaten sollte der Gesetzgeber absehen. Die Musik- und Filmindustrie sollte selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

10.1.4 Filterung von E-Mails zur Bekämpfung von Spam und zur Virenabwehr

Die Anzahl unverlangter Werbe-E-Mails („Spam“) ist im Laufe des zurückliegenden Berichtszeitraums weiter angestiegen: Für den November 2006 ermittelte das in Großbritannien ansässige Sicherheitsunternehmen MessageLabs eine Spam-Quote von weltweit 74 % (für Deutschland: 66,4 %)[136]. Vielfach werden über Spam-Mails auch Viren und andere Schadcodes verteilt. Zur Abwehr der damit verbundenen Behinderungen und Bedrohungen werden vielfach sowohl auf den Endgeräten der Nutzer als auch bei Anbietern von E-Mail-Diensten Spam-Filter eingesetzt.

Die Artikel-29-Datenschutzgruppe hat in ihrer Stel-

[135] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. EG L 201/37

[136] http://www.messagelabs.com/portal/server.pt/gateway/PTARGS_0_0_434_462_-462_43/http%3B/0120-0176-CTC1%3B8080/publishedcontent/publish/threat_watch_dotcom_de/intelligence_reports/november_2006/messagelabs_intelligence_report__november_2006_5.pdf

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

lungnahme 2/2006 Datenschutzfragen bei solchen Filterdiensten für elektronische Post behandelt[137]. Nach Auffassung der Arbeitsgruppe kann die Verwendung von Filtern für die Erkennung und weitere Behandlung virenbehafteter elektronischer Post grundsätzlich auf Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation[138] gestützt werden. Diese Vorschrift verpflichtet die Betreiber von Diensten der elektronischen Kommunikation, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten. Die Einrichtung von Filtersystemen durch die Anbieter elektronischer Dienste könne auch als Maßnahme betrachtet werden, mit der die Anbieter die Erfüllung des Dienstleistungsvertrages mit ihren Kunden sicherstellen. Diese erwarten, E-Mails mit einem gewissen Maß an Sicherheit empfangen und versenden zu können. Damit lasse sich die bei der Anwendung von Filtersystemen durch die Anbieter vorgenommene Datenverarbeitung auch nach Artikel 7 b der Datenschutzrichtlinie[139] rechtfertigen, nach der eine Verarbeitung von Daten erfolgen darf, wenn sie „erforderlich [ist] für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist." Die Arbeitsgruppe hat jedoch auch darauf hingewiesen, dass bei der Filterung durch die Anbieter bestimmte Regeln beachtet werden müssen: So müssen Inhalte von E-Mail-Nachrichten und etwaige beigefügte Anhänge geheimgehalten werden und dürfen außer an den bzw. die Empfänger an niemanden weitergegeben werden. Schließlich sollten die Nutzer über die Filtermaßnahmen informiert werden.

In Bezug auf Maßnahmen zum Filtern von elektronischer Post zur Aussortierung von Spam vertritt die Arbeitsgruppe die Auffassung, dass Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation auch auf diese Situation anwendbar sein könnte: Eine Bedrohung der allgemeinen Leistungsfähigkeit der E-Mail- und Netzdienste könnte es rechtfertigen, dass die Anbieter von Internet- und E-Mail-Diensten zum Schutz gegen Spam derartige Filterungen vornehmen. Die Arbeitsgruppe ist außerdem der Ansicht, dass eine solche Filterung auch durch Artikel 7 b der Datenschutzrichtlinie gerechtfertigt sein könnte, und begründet dies damit, dass eine Spamfilterung notwendig sein könnte, um den E-Mail-Anbieter in die Lage zu versetzen, den mit dem betroffenen Nutzer geschlossenen Dienstleistungsvertrag ordnungsgemäß zu erfüllen. Die Arbeitsgruppe hat jedoch auch hierzu Empfehlungen gegeben:

So sollten Teilnehmer eines Dienstes die Möglichkeit haben, sich gegen das Scannen ihrer E-Mails zum

[137] vgl. WP 118 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_de.pdf
[138] Richtlinie 2002/58/EG
[139] Richtlinie 95/46/EG

Herausfiltern von Spam zu entscheiden, und darüber hinaus in die Lage versetzt werden, die von den Filtereinrichtungen als Spam identifizierten E-Mails zu überprüfen, um zu verifizieren, ob es sich dabei tatsächlich um Spam handelt. Die Arbeitsgruppe unterstützt außerdem die Entwicklung von Filtersystemen, die die Nutzer entweder auf ihren Endgeräten oder auf Servern Dritter oder dem E-Mail-Server des Anbieters installieren und konfigurieren können und die es ihnen selbst ermöglichen festzulegen, welche Mitteilungen sie erhalten möchten und welche nicht.

Darüber hinaus nimmt die Arbeitsgruppe auch Stellung zu der Praxis einiger E-Mail-Anbieter, die sich das Recht auf das Durchsuchen oder sogar Beseitigen bestimmter unerwünschter Inhalte vorbehalten. Diese Praxis stellt nach Auffassung der Arbeitsgruppe einen Verstoß gegen Artikel 5 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation dar, soweit der Nutzer nicht seine Einwilligung hierzu erteilt hat oder den Anbietern entsprechende gesetzliche Verpflichtungen auferlegt worden sind.

Schließlich behandelt die Arbeitsgruppe Dienste, die es erlauben festzustellen, ob und wann eine verschickte E-Mail vom Empfänger bzw. den Empfängern gelesen wurde, ggf. auch wie oft sie gelesen bzw. geöffnet wurde, ob sie an andere weitergeleitet wurde und wenn ja, auf welchen E-Mail-Servern an welchem Standort. Damit lässt sich auch feststellen, welche Art von Webbrowser und Betriebssystem der Empfänger der E-Mail verwendet. Diese Datenverarbeitung erfolgt in der Regel stillschweigend, ohne dass die Empfänger der E-Mails darüber benachrichtigt oder darauf hingewiesen werden. Sie haben auch keine Wahlmöglichkeit, die beschriebene Verarbeitung zu akzeptieren oder abzulehnen. Gegen diese Art der Verarbeitung spricht sich die Gruppe mit Nachdruck aus, soweit nicht die Empfänger zweifelsfrei ihre Einwilligung hierzu gegeben haben.

Die Filterung von E-Mails zur Bekämpfung von Spam und zur Virenabwehr kann unter bestimmten Umständen auf die Vorschriften der Datenschutzrichtlinie für elektronische Kommunikation gestützt werden. Dabei sind Systeme vorzuziehen, bei denen die Filterung unter der Kontrolle des Empfängers erfolgt. Weiter gehende Inhaltskontrollen sind ohne Einwilligung der Betroffenen unzulässig, ebenso Dienste, die eine Verfolgung des Umgangs mit einer Nachricht durch den Empfänger ermöglichen.

10.1.5 Automatische Notrufe im Falle eines Unfalles – „eCall“

Die Europäische Union plant gegenwärtig die Einführung eines harmonisierten Verfahrens für *Notrufe*, die durch in den Fahrzeugen installierte Geräte bei Unfällen an die zuständige Rettungsleitstelle abgesetzt werden sollen („eCall“). Dabei handelt es sich um eine

von mehreren Initiativen der Europäischen Kommission im Rahmen des eSafety-Forums, einer gemeinsamen Initiative des öffentlichen und privaten Sektors zur Verbesserung der Sicherheit im Straßenverkehr durch Nutzung von „fortgeschrittenen“ Informations- und Kommunikationstechnologien.

Für die Einführung des eCall-Verfahrens ist eine Steuerungsgruppe gegründet worden, die aus Vertretern der verschiedenen Interessengruppen besteht. Die Steuerungsgruppe hat ein Memorandum of Understanding erarbeitet, das bereits im August 2004 von der Europäischen Kommission und weiteren Partnern unterzeichnet wurde. Bis zum September 2006 hatten mehr als 60 Institutionen einschließlich sieben Mitgliedstaaten der Europäischen Union sowie die Schweiz und Norwegen das Memorandum unterzeichnet. Deutschland gehört gegenwärtig nicht zu den Signataren. Das eCall-Verfahren basiert auf einer technischen Einrichtung, die nach Vorstellung der Steuerungsgruppe ab dem 1. September 2010 in alle in der Europäischen Union neu gebauten Fahrzeuge integriert werden soll. Bei einem Unfall soll diese Einrichtung unter Nutzung verschiedener im Fahrzeug befindlicher Sensoren automatisch eine Telefonverbindung zur nächstgelegenen Rettungsleitstelle aufbauen. Dabei soll gleichzeitig ein Minimaldatensatz übertragen werden, der bestimmte Grunddaten u. a. zur Beschreibung des Unfalls, des beteiligten Fahrzeuges und dessen Standort enthält. Der Anruf kann von den Fahrzeuginsassen auch manuell ausgelöst werden.

Die Artikel-29-Datenschutzgruppe hat im September 2006 ein Arbeitspapier zu den Datenschutzimplikationen dieser Initiative verabschiedet[140]. Dabei hat sie insbesondere darauf hingewiesen, dass es von großer Bedeutung ist, ob ein solches System verpflichtend in allen Fahrzeugen eingebaut und aktiviert wird oder ob dies nur auf ausdrücklichen Wunsch der jeweiligen Nutzer geschehen soll. Soweit die Inanspruchnahme dieses Dienstes freiwillig ist, muss nach Auffassung der Arbeitsgruppe eine einfache Möglichkeit zum Aktivieren bzw. Deaktivieren dieser Einrichtung eingeführt werden. Der Nutzer (der nicht notwendigerweise der Besitzer des Fahrzeugs sein muss) solle jederzeit die Möglichkeit haben, das System ohne jegliche technische oder finanzielle Beschränkung ein- und auszuschalten. Die Arbeitsgruppe hat ausdrücklich begrüßt, dass nach Aussagen der Projektgruppe das System so ausgestaltet werden soll, dass eine permanente Geolokalisierung von Fahrzeugen schon technisch nicht möglich ist, weil sich die im Fahrzeug befindliche Einrichtung erst in ein Kommunikationsnetz einbuchen soll, wenn sie durch einen Unfall oder manuell durch die Fahrzeuginsassen aktiviert wird.

[140] Working document on data protection and privacy implications in eCall initiative (WP 125) v. 26. September 2006; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_de.pdf

Soweit ein solches System verpflichtend eingeführt werden soll, hat die Arbeitsgruppe darauf hingewiesen, dass es hierzu einer EU-weiten spezifischen Rechtsvorschrift bedürfte. Eine solche Rechtsvorschrift müsste den in der Datenschutzrichtlinie 95/46/EG festgelegten Kriterien wie z. B. dem Prinzip der Verhältnismäßigkeit genügen.

Die Arbeitsgruppe hat jedoch klargestellt, dass sie die freiwillige Nutzung eines solchen Systems gegenüber dessen verpflichtender Einführung bevorzugt.

Systeme für automatische *Notrufe* bei Unfällen sollten nur aufgrund der freiwilligen Entscheidung der Nutzer eingeführt werden. Die Systeme sind so auszugestalten, dass die Nutzer jederzeit die Möglichkeit haben, sie ohne technische oder finanzielle Beschränkungen ein- und auszuschalten. Eine permanente Geolokalisierung von Fahrzeugen darf schon technisch nicht möglich sein.

10.1.6 Novellierung des Telekommunikationsgesetzes

Im Mai 2006 hat die Bundesregierung den Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften vorgelegt[141]. Mit der beabsichtigten Änderung des Telekommunikationsgesetzes (TKG) werden zunächst die Vorschriften der bisherigen Telekommunikations-Kundenschutzverordnung[142] in das TKG integriert. Daneben werden zwei Vorschriften der Datenschutzrichtlinie für elektronische Kommunikation[143] in nationales Recht umgesetzt: So sollen die Informationspflichten der Diensteanbieter, nach § 93 TKG durch eine Regelung ergänzt werden, die den Anbietern zusätzlich zu den bestehenden Informationspflichten eine Information der Teilnehmer über besondere Risiken der Verletzung der Netzsicherheit und mögliche Abhilfen einschließlich voraussichtlich entstehender Kosten auferlegt[144].

Die Vorschrift zur Verarbeitung von Standortdaten in § 98 TKG soll um einen Absatz ergänzt werden, der eine Zweckbindung der Verarbeitung von Standortdaten in dem für die Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß vorsieht. Die Verarbeitung ist darüber hinaus auf Personen zu beschränken, die im Auftrag des Netzbetreibers oder des Dienstanbieters[145] tätig sind.

---

[141] BR-Drs. 359/06

[142] TKV v. 11. Dezember 1997, BGBl. I, 2910, zuletzt geändert durch Artikel 22 des Gesetzes zur Anpassung von Verjährungsvorschriften an das Gesetz zur Modernisierung des Schuldrechts v. 9. Dezember 2004, BGBl. I, 3214

[143] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. EU L 2001/37

[144] vgl. Artikel 4 Abs. 2 Richtlinie 2002/58/EG

[145] vgl. Artikel 9 Abs. 3 Richtlinie 2002/58 EG

Schließlich wird die Vorschrift über Einzelverbindungsnachweise aus § 99 Absatz 1 Satz 1 TKG so ergänzt, dass Diensteanbieter dem Teilnehmer auf dessen Wunsch auch die Daten pauschal abgegoltener Verbindungen auf dem Einzelverbindungsnachweis mitteilen dürfen.

Das Gesetzgebungsverfahren war bis zum Ende des Berichtszeitraums noch nicht abgeschlossen.

10.1.7 Internationales Symposium „Datenschutz und Datensicherheit bei *Internet-Telefonie/Voice oder IP*“

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat wiederum im Rahmen der Internationalen Funkausstellung ein internationales Symposium veranstaltet. Thema der diesjährigen Veranstaltung waren der Datenschutz und die Datensicherheit bei Angeboten zur Internet-Telefonie. Das Telefonieren über das Internet gewinnt zunehmend an Bedeutung. Bereits jetzt sind Angebote auf dem Markt verfügbar, die einen vollständigen Ersatz von Festnetzanschlüssen durch Angebote zur Internet-Telefonie auf der Basis bestehender Breitbandkabel- oder DSL-Anschlüsse ermöglichen. Auch Betriebe und Einrichtungen der öffentlichen Verwaltung ersetzen oder ergänzen ihre Telefonanlagen zunehmend durch solche „Voice over IP“-Anwendungen. Bei dem Symposium diskutierten internationale Experten aus Wissenschaft, Wirtschaft und Verwaltung, welche Risiken diese Entwicklung ggf. für den Datenschutz, die Datensicherheit oder den Bestand des Fernmeldegeheimnisses birgt. Dabei wurde auch erörtert, ob die Vertraulichkeit der Kommunikation in dem unsicheren Medium Internet überhaupt wirksam sichergestellt und wie die Einhaltung von Schutzbestimmungen grenzüberschreitend kontrolliert werden kann. Schließlich wurde die Fragestellung behandelt, ob die Einführung der neuen Verfahren im Vergleich zur traditionellen Telefonie unter Umständen auch neue Möglichkeiten für eine datenschutzgerechte Ausgestaltung von Kommunikationsangeboten bietet. Materialien zu den Vorträgen der einzelnen Referenten können in unserem Internetangebot abgerufen werden[146].

10.2 Tele- und Mediendienste

10.2.1 Entwurf für ein *Telemediengesetz*

Über die Vorbereitung zu dieser Gesetzgebungsinitiative, mit der die bisher bestehenden unterschiedlichen Rechtsvorschriften für Informations- und Kommunikationsdienste bei weitgehender Beibehaltung des materiellen Rechts zusammengefasst werden sol-

[146] vgl. http://www.datenschutz-berlin.de/aktuelle/termine/06/bln/symposium_2006.htm

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

len, hatten wir bereits in unserem Jahresbericht 2005 ausführlich berichtet[147]. Auf der Basis der dort geschilderten Vorarbeiten hat die Bundesregierung nunmehr im zurückliegenden Berichtszeitraum einen entsprechenden Gesetzentwurf vorgelegt[148].

Zusätzlich zu den bereits in unserem Jahresbericht 2005 dargestellten materiellen Rechtsänderungen enthält der Entwurf folgende weitere Änderungen des geltenden Rechts:

Versendern kommerzieller Kommunikation per elektronische Post wird untersagt, den Absender oder den kommerziellen Charakter der Nachricht zu verschleiern oder zu verheimlichen. Ein Verstoß gegen diese Vorschrift ist bußgeldbewehrt (§§ 6 Abs. 2 sowie 16 Abs. 1 des Entwurfs).

Bestands- und Nutzungsdaten sollen zukünftig grundsätzlich auch für Zwecke der Gefahrenabwehr zur Verfügung stehen. Der Bundesrat hat in seiner Stellungnahme gefordert, die Auskunftsvorschrift zu Bestandsdaten in § 14 Abs. 2 des Entwurfs auch zur Gefahrenabwehr durch die Polizeibehörden der Länder zu ermöglichen. Dies hat er damit begründet, dass Bestands- und Nutzungsdaten von Telemedien-Diensten auch zur Gefahrenabwehr, die auch die vorbeugende Bekämpfung von Straftaten umfasst, benötigt würden[149]. Der Bedarf an einer solchen Erweiterung ist allerdings nicht hinreichend nachgewiesen. Die Begründung zu der Änderung nennt lediglich ein hypothetisches Beispiel. Umso erstaunlicher ist es, dass die Bundesregierung in ihrer Gegenäußerung[150] dieser Erweiterung einfach zugestimmt hat.

Insgesamt bestehen auch Zweifel, ob die von der Bundesregierung angestrebte „... verbesserte Abgrenzung des Telemedien-Datenschutzes gegenüber dem Telekommunikationsdatenschutz ..."[151] gelungen ist. Nicht ausgeräumt sind jedenfalls die von uns bereits im Jahresbericht 2005 beschriebenen Probleme hinsichtlich der Kontrollzuständigkeit.

Die Regelungen des Telemediengesetzes sollen auch im Bereich des Rundfunks Anwendung finden: Im Berichtszeitraum sind die Arbeiten am 9. Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (9. Rundfunkänderungsstaatsvertrag) abgeschlossen worden. Der Vertrag wurde im Sommer 2006 von den Ministerpräsidenten der Länder unterzeichnet. Nach Ratifizierung durch die Landesparlamente soll der

147 JB 2005, 5.2

148 Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – EIGVG), BR-Drs. 556/06

149 BR-Drs. 556/06 (Beschluss), unter Nr. 5

150 BT-Drs. 16/3135

151 vgl. Gesetzentwurf der Bundesregierung, BT-Drs. 16/3135, 2 (unter B.)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Staatsvertrag am 1. März 2007 in allen Ländern gleichzeitig in Kraft treten. Die bisher in den §§ 47 a–f enthaltenen Vorschriften zum Datenschutz für Veranstalter von Rundfunk sind durch einen Verweis auf die Vorschriften des Abschnittes „Datenschutz“ des Telemediengesetzes „in der jeweils geltenden Fassung“ ersetzt worden[152]. Ziel der Änderung ist eine Vereinheitlichung der Datenschutzvorschriften im Bereich des Rundfunks sowie bei den Tele- und Mediendiensten.

Darüber hinaus hat der Senat von Berlin im Oktober 2006 dem Abgeordnetenhaus einen Dritten Staatsvertrag zur Änderung des Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks vorgelegt[153]. Dort ist u. a. vorgesehen, die bisher in dem Staatsvertrag enthaltenen Regelungen zum Datenschutz zu streichen und durch einen Verweis auf die entsprechenden Regelungen im Rundfunkstaatsvertrag zu ersetzen. Durch den dortigen Verweis auf die Datenschutzvorschriften des Telemediengesetzes würden dessen Datenschutzvorschriften dann auch für private Rundfunkveranstalter in Berlin und Brandenburg gelten.

Das neue Telemediengesetz darf hinsichtlich des Datenschutzes nicht hinter den Regelungen der bisher geltenden Rechtsvorschriften zurückbleiben. Zusätzliche Öffnungsklauseln, die Geheimdiensten oder sogar privaten Dritten den Zugriff auf Nutzungsdaten ermöglichen, sollten nicht in das Gesetz aufgenommen werden. Insbesondere sollte auf ein Auskunftsrecht der Polizeibehörden der Länder für Bestands- und Nutzungsdaten für Zwecke der Gefahrenabwehr verzichtet werden, solange die Notwendigkeit für die Schaffung einer solchen Vorschrift nicht schlüssig nachgewiesen ist.

10.2.2 Personenbezogene Daten im *„Cache“* von *Suchmaschinen*

Verschiedentlich haben sich Betroffene im zurückliegenden Berichtszeitraum an uns gewandt, deren personenbezogene Daten aus einem Internet-Angebot gelöscht wurden, aber über in Suchmaschinen gespeicherte Kopien der ursprünglich veröffentlichten Seiten nach wie vor im Internet verfügbar waren.

Einige Suchmaschinen kopieren bei der Indexierung von Internet-Angeboten Inhalte aus diesen Angeboten und stellen diese „Schnappschüsse“ als Teil des Suchmaschinenangebots zum Abruf zur Verfügung („Cache“). Dies wird damit begründet, dass solche Kopien auch dann zum Abruf bereitgestellt werden können, wenn das ursprüngliche Angebot gerade nicht verfügbar ist. Werden nun personenbezogene Daten

[152] vgl. die Neufassung des § 47 Abs. 1, Nr. 14 der Anlage zu Abghs.-Drs. 16/0026
[153] Abghs.-Drs. 16/0076

aus dem ursprünglichen Angebot gelöscht, kann es vorkommen, dass diese Kopien weiterhin im Internet für allgemeinen Zugriff zur Verfügung stehen. Obwohl viele Betreiber von Suchmaschinen angeben, ihre Indexeinträge regelmäßig und in kurzen Abständen zu aktualisieren, sind in einigen Fällen Kopien auch weit zurückliegender und längst im ursprünglichen Angebot gelöschter Einträge verfügbar.

Hierzu ist aus Datenschutzsicht Folgendes zu bemerken: Die Art und Weise, wie Angebote durch Suchmaschinen indexiert werden, kann zunächst vom Anbieter der ursprünglichen Website selbst beeinflusst werden. Dieser muss abwägen, inwieweit eine Indexierung der personenbezogenen Daten in seinem Angebot und das Anlegen von Kopien bei den Betreibern von Suchmaschinen von dem ursprünglichen Verarbeitungszweck umfasst bzw. durch eine ggf. vorliegende Einwilligung der Betroffenen gedeckt sind. Soweit dies nicht der Fall ist, hat der Anbieter durch entsprechende Ausgestaltung seines Angebots dafür Sorge zu tragen, dass die Indexierung bzw. Anfertigung von Kopien durch Anbieter von Suchmaschinen für sein Angebot oder Teile dieses Angebots unterbleibt[154].

Einige Anbieter von Suchmaschinen bieten den Betroffenen selbst die Möglichkeit, auch eine Entfernung von personenbezogenen Daten aus veralteten Kopien zu veranlassen, die bei den Anbietern von Suchmaschinen gespeichert werden. Dies ist zu begrüßen. Anbieter mit Sitz in Deutschland sind hierzu ohnehin nach dem Bundesdatenschutzgesetz verpflichtet.

Schließlich sollten sich auch die Betroffenen selbst fragen, inwieweit sie die Risiken, die mit der Veröffentlichung von personenbezogenen Daten im Internet verbunden sind, überhaupt in Kauf nehmen wollen. Die Verwendung personenbezogener Daten kann, nachdem sie einmal im Internet veröffentlicht worden sind, praktisch nicht mehr kontrolliert werden. Nicht nur Betreiber von Suchmaschinen, sondern auch andere, beliebige Dritte können Kopien der veröffentlichten Daten fertigen und diese unkontrolliert weiterverarbeiten und nutzen. Insoweit ist bei der Veröffentlichung personenbezogener Daten im Internet größte Zurückhaltung geboten. Die Löschung einmal veröffentlichter personenbezogener Daten im Internet kann ausgesprochen mühsam sein und in manchen Fällen – sofern die unbefugte Speicherung und/oder Weiterverwendung überhaupt bemerkt wird – auch unter Einschaltung von Datenschutzaufsichtsbehörden nur schwer oder sogar überhaupt nicht durchgesetzt werden, z. B. wenn sich der Anbieter im Ausland befin-

[154] Hierzu kann im Wurzelverzeichnis des Angebots eine Datei mit dem Namen „robots.txt“ angelegt und mit entsprechenden Einträgen versehen werden. Zwar handelt es sich bei diesem Protokoll um eine Konvention, deren Einhaltung nicht erzwungen werden kann. Nach hiesiger Kenntnis respektieren Anbieter von Suchmaschinen jedoch in der Regel die dort spezifizierten Regelungen zur Indexierung der Angebote.

det.

Der Umfang der Indexierung durch Suchmaschinen muss mit dem ursprünglichen Zweck der Verarbeitung personenbezogener Daten auf der jeweiligen Website vereinbar sein. Betroffene sollten die Veröffentlichung ihrer personenbezogenen Daten im Internet auf ein Minimum beschränken.

10.2.3 Datenschutz bei *Suchmaschinen*

Auf unseren Vorschlag hin hat die 28. Internationale Konferenz der Datenschutzbeauftragten am 3. November 2006 in London eine Entschließung zu Datenschutz bei Suchmaschinen gefasst[155]. Darin werden die Anbieter von Suchmaschinen u. a. aufgefordert, künftig nach dem Ende der Nutzung keine personenbezogenen Daten über Suchanfragen (z. B. IP-Adressen) mehr zu speichern. Auf diese Weise soll auch verhindern werden, dass personenbezogene Daten der Nutzer von Suchmaschinen dem Zugriff Dritter ausgesetzt sind. Hintergrund ist die Veröffentlichung von nahezu 20 Millionen scheinbar anonymisierten Suchanfragen durch den Internet-Anbieter AOL im Sommer 2006 in den USA. Bereits im Frühjahr 2006 hatte das Justizministerium der Vereinigten Staaten von Amerika von dem Betreiber der Suchmaschine „Google“ die Herausgabe von Millionen von Suchanfragen im Zusammenhang mit einem Gerichtsverfahren verlangt.

Anbieter von Suchmaschinen sollten nach dem Ende der Nutzung keine personenbezogenen Daten über Suchanfragen (z. B. IP-Adresse) speichern, soweit dies nicht für die Erbringung weiterer Dienste gegenüber dem Nutzer erforderlich ist und dieser freiwillig eine informierte Einwilligung dazu erteilt hat.

10.2.4 *Weblogs* und Online-Communities

Zwei webbasierte Internet-Dienste führen aufgrund ihrer zunehmenden Verbreitung und Nutzung zu einer höheren Bedeutung der mit ihnen verbundenen datenschutzrechtlichen Fragen: *Weblogs* (kurz: *Blogs*) sowie *Online-Communities* (soziale Netzwerke).

Ein *Weblog* ist eine WWW-Seite, die von ihrem Betreiber, dem *Blogger*, regelmäßig aktualisiert wird und Beiträge in Form eines Tagebuchs über das Leben des Bloggers oder zu einem Thema allgemeinen Interesses enthält, die meist von Lesern der WWW-Seite durch Kommentare ergänzt werden können. Datenschutzrechtlich interessant und nicht allgemein zu beantworten ist die Frage, ob der Blogger ähnlich wie Presse und Medien bei der Veröffentlichung von Informati-

[155] vgl. http://www.datenschutz-berlin.de/doc/int/konf/28/Entschliessung%20zum%20datenschutz%20bei%20Suchmaschine.pdf, Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 98

onen über einzelne Personen ein *„Medienprivileg“* beanspruchen kann oder uneingeschränkt den Regelungen des Bundesdatenschutzgesetzes unterliegt.

Eine *Online-Community* besteht aus einer meist offenen Gruppe von Computeranwendern, die sich über ein WWW-Forum oder ein Chat-Forum kennen lernt und über ein bestimmtes Thema Meinungen und Informationen austauscht. Da in Online-Communities neben einer Vielzahl von Nutzerprofilen mit teilweise sehr persönlichen Angaben über die Angehörigen der Community auch aus deren Textbeiträgen sehr detaillierte Informationen zusammengetragen werden können, ist von besonderem datenschutzrechtlichem Interesse, wie die meist freiwillig veröffentlichten Informationen davor geschützt werden können, von Dritten für andere Zwecke zusammengeführt und ausgewertet zu werden.

Eine interessante Konstellation von Weblogs und Online-Community beschäftigte uns in den letzten Wochen des Jahres 2006: Blogger veröffentlichten eine Reihe von Hinweisen auf technische Sicherheitsmängel der WWW-Seiten einer großen deutschen Online-Community von ca. einer Million Studierenden, die von der Berliner Firma StudiVZ betrieben wird.

Eine datenschutzrechtliche Kontrolle von StudiVZ nach § 38 BDSG bestätigte, dass es durch Fehler im Entwurf und der Implementierung der für die WWW-Seiten des Portals *studivz.net* verwendeten Server-Software möglich war, ohne großen Aufwand an Informationen über einzelne Studierende zu gelangen, die von den Betroffenen vermeintlich nur einem beschränkten Benutzerkreis zugänglich gemacht worden waren. Auf diese Weise war es einem Blogger gelungen aufzudecken, dass eine Gruppe von StudiVZ-Nutzern ein *„Online-Stalking“* von Studentinnen betrieb, die ein Foto von sich in ihrem Nutzerprofil gespeichert hatten. Die Persönlichkeitsrechte der Studentinnen wurden dadurch teilweise massiv verletzt.

Zudem war es möglich, eine große Zahl von Benutzerprofilen automatisiert auszulesen und die personenbezogenen Daten für eigene Zwecke zu verwenden. Auf dem 23. Chaos Computer Congress im Dezember 2006 (23C3) wurde beispielsweise eine statistische Auswertung der StudiVZ-Daten inklusive der Beziehungen der StudiVZ-Nutzer untereinander veröffentlicht[156]. In dem Bericht wurde allerdings eingeräumt, dass die Betreiber von StudiVZ mittlerweile technische Maßnahmen ergriffen haben, um den automatisierten missbräuchlichen Abruf von Nutzerprofilen deutlich zu erschweren.

Zum Zeitpunkt unserer Kontrolle waren die Betreiber von StudiVZ zudem bereits damit beschäftigt, die auf-

[156] vgl. http://studivz.irgendwo.org/

gedeckten Fehler ihrer Software zu beseitigen. Zeitweise war das Online-Angebot *studivz.net* zu diesem Zweck mehrere Tage lang abgeschaltet. Als hauptsächlicher Grund für die vielen, teilweise gravierenden Fehler der Software wurde angegeben, dass die Betreiber des als studentisches Projekt initiierten Angebots *studivz.net* den durch das enorme Wachstum der Nutzerzahl veränderten Anforderungen zeitweise nur unzureichend genügen konnten und eine umfassende Fehlerkorrektur trotz großer Bemühungen nicht möglich war. Aus datenschutzrechtlicher Sicht ist diese Begründung unzureichend, weil die technischen Grundlagen bereits zum Zeitpunkt der Freischaltung des Angebots und der Speicherung der ersten personenbezogenen Daten zeitgemäßen Anforderungen hätten genügen müssen.

Neben der Beseitigung der technischen Mängel des Systems wird unter anderem die Datenschutzerklärung des Online-Angebots überarbeitet und es sind weitere datenschutzrechtliche Fragen zu klären. Es ist damit zu rechnen, dass dieser Vorgang uns bis weit in das Jahr 2007 hinein beschäftigt. Gegen Ende des Berichtszeitraums wurde StudiVZ von einem großen Verlagshaus übernommen. Das zeigt, welche wirtschaftliche Bedeutung Online-Communities mittlerweile haben. An unserer Zuständigkeit als Aufsichtsbehörde für StudiVZ ändert sich nichts, denn der Betreiber dieser Online-Community bleibt datenschutzrechtlich verantwortliche Stelle.

Weblogs und *Online-Communities* werfen neuartige datenschutzrechtliche Fragen auf, die noch nicht abschließend beantwortet werden können. Die technische Realisierung dieser webbasierten Dienste muss sorgfältig konzipiert und umgesetzt werden, um gravierende Gefährdungen für die Privatsphäre der Nutzer zu vermeiden.

10.3 Medien

10.3.1 Verfahren zur Befreiung von der *Rundfunkgebührenpflicht*

Bereits in unserem letzten Jahresbericht hatten wir Hinweise zu den Rechten der Betroffenen beim Verfahren zur Befreiung von der Rundfunkgebührenpflicht gegeben[157].

Um die bisher vorhandenen Defizite auszuräumen, sind im zurückliegenden Berichtszeitraum Gespräche zwischen Vertretern der Datenschutzbeauftragten, der behördlichen Datenschutzbeauftragten der Landesrundfunkanstalten und der Landesregierungen geführt worden. Ziel dieser Gespräche war eine Vereinfachung des Antragsverfahrens bei der Befreiung von der Rundfunkgebühr, um einen besseren Schutz der

[157] JB 2005, 5.3

Privatsphäre der Betroffenen zu gewährleisten, als dies gegenwärtig der Fall ist. Insbesondere soll zukünftig auf die Erhebung solcher Daten durch die *Gebühreneinzugszentrale* (GEZ) verzichtet werden, die für die Befreiung von der Rundfunkgebühr nicht erforderlich sind. Hierzu ist gegenwärtig geplant, dass Beziehern von Arbeitslosengeld II, die einen großen Prozentsatz derjenigen darstellen, die von der Rundfunkgebühr befreit werden können, von den Jobcentern als Anlage zu dem Bescheid über Arbeitslosengeld II eine Bescheinigung ausgedruckt wird, die nur die für die Befreiung von der Rundfunkgebühr notwendigen Daten enthält. Bereits jetzt akzeptiert die GEZ sog. „Drittbescheinigungen" z. B. der Sozialleistungsträger, soweit diese die für die Bearbeitung eines Antrags auf Befreiung von der Rundfunkgebühr erforderlichen Daten enthalten.

10.3.2 Rundfunkgebühr für internetfähige PCs

Zum 31. Dezember 2006 lief eine Übergangsbestimmung aus dem Rundfunkgebührenstaatsvertrag aus, nach der Gebühren für Rechner, die Rundfunkprogramme ausschließlich über Angebote aus dem Internet wiedergeben können, nicht zu entrichten waren[158]. Damit ist ab dem 1. Januar 2007 eine Rundfunkgebühr auch dann zu entrichten, wenn zwar keine klassischen Rundfunkempfangsgeräte wie Radios oder Fernseher, aber internetfähige PCs oder andere internetfähige Endgeräte (z. B. Handys) „zum Empfang bereitgehalten werden". Diese Regelung hatte zu einer erregten öffentlichen Diskussion geführt. Insbesondere Gewerbetreibende, die bisher mangels vorhandener Rundfunkgeräte nicht zur Zahlung einer Rundfunkgebühr verpflichtet waren, aber über internetfähige Rechner verfügen, hatten kritisiert, dass auch sie zu-künftig zur Zahlung einer Gebühr herangezogen werden sollen. Demgegenüber verwiesen die Rundfunkanstalten darauf, dass Programme öffentlich-rechtlicher Sender zunehmend auch über das Internet verbreitet würden und deshalb für diese Empfangsmöglichkeit eine Gebühr zu entrichten sei.

Im Zuge der Konvergenz der verschiedenen Dienste (Rundfunk, Internet, Telekommunikation) ist damit zu rechnen, dass zukünftig auch Inhalte öffentlich-rechtlicher Rundfunkanstalten verstärkt medienübergreifend zur Verfügung gestellt werden. Diese Entwicklung macht einmal mehr deutlich, dass das „Bereithalten eines Rundfunkgeräts zum Empfang", das gegenwärtig den Anknüpfungspunkt für die Rundfunkgebührenpflicht bildet, in dieser Form zukünftig nicht sinnvoll aufrechterhalten werden kann, weil praktisch jede und jeder über mindestens ein Endgerät verfügen wird, das zumindest theoretisch den Zugang

[158] vgl. § 11 Rundfunkgebührenstaatsvertrag; Artikel 4 des Staatsvertrages über den Rundfunk im Vereinten Deutschland v. 31. August 1991, zuletzt geändert durch den 8. Rundfunkänderungsstaatsvertrag v. 8.–15. Oktober 2004

auch zu Inhalten öffentlich-rechtlicher Sender ermöglicht. Im Gegensatz zu den speziellen Rundfunk- und Fernsehgeräten werden aber Computer und Handys immer noch vorwiegend für andere Zwecke genutzt.

Konsequenterweise sind im Zuge der Debatte über die Einführung der Rundfunkgebühr für PCs aus dem politischen Raum wiederum Forderungen laut geworden, das gegenwärtige System zu überarbeiten und die gegenwärtige Gebühr durch eine Abgabe zu ersetzen, die unabhängig davon gezahlt werden soll, ob Rundfunkempfangsgeräte vorhanden sind oder nicht.

Für den Datenschutz hätte dies den Vorteil, dass damit die bundesweit einmalige Sammlung personenbezogener Daten von Rundfunkteilnehmern, die gegenwärtig durch die GEZ in Köln gespeichert und verarbeitet werden, entbehrlich werden könnte. Auch die von uns wiederholt kritisierten Übermittlungen aus dem Melderegister an die Landesrundfunkanstalten zur Feststellung der Gebührenpflicht könnten entfallen. Schließlich würde auch die Tätigkeit der sog. „Rundfunkgebührenbeauftragten“ entbehrlich, die die Betroffenen zu Hause aufsuchen, um das Vorhandensein oder Nichtvorhandensein einer Rundfunkgebührenpflicht festzustellen.

Bereits in unserem Jahresbericht 1999 hatten wir die damaligen Überlegungen zur Abschaffung der gerätebezogenen Rundfunk- und Fernsehgebühr unterstützt[159].

Die gerätebezogene Rundfunk- und Fernsehgebühr sollte mittelfristig durch ein System ersetzt werden, bei dem auf die Verarbeitung personenbezogener Daten von Rundfunkteilnehmern im bisherigen Umfang verzichtet werden kann.

10.4 Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation

Die Arbeitsgruppe hat auf ihren turnusmäßigen halbjährlichen Treffen unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit drei Arbeitspapiere verabschiedet:

- Das Arbeitspapier zur Online-Verfügbarkeit elektronischer Gesundheitsdaten enthält Empfehlungen zur datenschutzgerechten Ausgestaltung der Verarbeitung elektronischer Gesundheitsdaten in Kommunikationsnetzen[160].

- Das Arbeitspapier zu Datenschutz und Datensicherheit bei der *Internet-Telefonie* weist auf das Erfordernis hin, sicherzustellen, dass der existierende Regulierungsrahmen auf nationaler und internationaler

[159] vgl. JB 1999, 5.3

[160] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 112

Ebene zur Wahrung des Fernmeldegeheimnisses auch auf diese Dienste erstreckt wird. Anbieter von Internet-Telefonie sollten verpflichtet sein, als ein Minimum denselben Grad von Datensicherheit und Schutz der Privatsphäre anzubieten wie ein „traditioneller“ Festnetz- und Mobiltelefondienst. Das Arbeitspapier enthält darüber hinaus detaillierte Anforderungen an Hersteller und Anbieter von Internet-Telefonie-Diensten zur Gewährleistung von Datenschutz und Datensicherheit[161].

- Im Hinblick auf das „Trusted Computing“ und die damit zusammenhängenden Technologien zur digitalen Rechteverwaltung hat die Arbeitsgruppe in einem weiteren Arbeitspapier darauf hingewiesen, dass der Einsatz dieser Technologie durch öffentliche Stellen unter bestimmten Umständen mit Rechten der Betroffenen (z. B. dem Recht auf Auskunft über ihre gespeicherten personenbezogenen Daten) kollidieren kann. Die Arbeitsgruppe empfiehlt, dass Regierungen die potenziellen Gefahren für den Datenschutz und die Langzeitverfügbarkeit offizieller Dokumente in Betracht ziehen sollten, die aus der Einführung dieser Technologien resultieren können. Sie verweist auf eine Veröffentlichung der neuseeländischen Regierung, in der diese Risiken und mögliche Abhilfen detailliert beschrieben werden[162].

Darüber hinaus hat die Arbeitsgruppe ihren gemeinsamen Standpunkt zum Datenschutz bei Suchmaschinen im Internet von 1998 überarbeitet und aktualisiert. In dieser überarbeiteten Fassung wird insbesondere die Notwendigkeit der datenarmen Gestaltung von Suchmaschinenangeboten betont. Zudem werden die Anbieter von Suchmaschinen aufgefordert, den Betroffenen eine Möglichkeit einzuräumen, veraltete Kopien ihrer personenbezogenen Daten löschen zu lassen, die bei den Anbietern von Suchmaschinen in einem sog. „Cache“ gespeichert sind[163].

11 *Informationsfreiheit*

11.1 Informationsfreiheit auf Bundesebene

Am 1. Januar ist das *Gesetz zur Regelung des Zugangs zu Informationen des Bundes*[164] in Kraft getreten. Die Bundesrepublik ist damit im europäischen Ländervergleich endlich nicht mehr Schlusslicht. Dass der Bedarf an mehr Transparenz auch in den Bundesbehörden immens ist, belegen die statistischen Erhebungen

[161] vgl. Anlagenband, a.a.O., S. 118
[162] vgl. Anlagenband, a.a.O., S. 121
[163] vgl. Anlagenband, a.a.O., S. 115
[164] v. 5. September 2005, BGBl. I, 2722

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

nach knapp sechs Monaten.[165] Bei ca. 330 bearbeiteten Anträgen wurde in mehr als 60 % der Informationszugang zumindest teilweise gewährt. Der Bundesbeauftragte für den Datenschutz, der nun zugleich Bundesbeauftragter für die Informationsfreiheit ist, musste in ca. 140 Fällen seiner Schiedsstellenfunktion nachkommen. Bis zum Jahresende gingen insgesamt fast 200 schriftliche Beschwerden bei ihm ein[166]. Die meisten IFG-Anträge wurden beim Auswärtigen Amt und beim Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz gestellt.

Wahrscheinlich waren die hohe Zahl der dort gestellten IFG-Anträge sowie die sog. Gammelfleisch-Skandale mitursächlich dafür, dass nach erfolglosen Anläufen in den Jahren 2001 und 2004 ein *Gesetz zur Neuregelung des Rechts der Verbraucherinformationen* auf den Weg gebracht wurde. Es sollte neben Änderungen des Lebensmittel- und Futtermittelgesetzbuches und des Weingesetzes ein eigenes Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (Verbraucherinformationsgesetz – VIG) enthalten. Damit wäre dem berechtigten Interesse der Verbraucher an einer besseren Transparenz bei Lebensmitteln und Bedarfsgegenständen Rechnung getragen worden, indem der Zugang zu den bei den Behörden des Bundes, der Länder und der Gemeinden vorhandenen Informationen eröffnet worden wäre. Die Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland (AGID) hatte in einer Entschließung gleichwohl Verbesserungen angemahnt und gefordert, dass das Gesetz nicht nur auf Lebens- und Futtermittel, sondern auch auf sonstige Produkte und Dienstleistungen angewendet und ein unmittelbarer Rechtsanspruch auf Informationszugang bei Unternehmen geschaffen wird[167]. Leider wurde das Gesetz vom Bundespräsidenten nicht ausgefertigt, sodass es nicht in Kraft getreten ist. Er hatte verfassungsrechtliche Bedenken angemeldet, weil nach der Föderalismusreform eine Übertragung von neuen Aufgaben auf die Gemeinden und Gemeindeverbände durch Bundesgesetz nicht erfolgen darf. Ob ein neuer bundesgesetzgeberischer Anlauf vor diesem Hintergrund erfolgt oder die Landesgesetzgeber gefordert sind, bleibt abzuwarten. In Berlin wäre jedenfalls das bereits vorhandene Verbraucherinformationsgesetz um einen eigenen Informationsanspruch der Verbraucher zu ergänzen[168].

---

[165] vgl. Antwort der Bundesregierung auf die Kleine Anfrage u. a. der FDP-Fraktion: Probleme bei der Anwendung des Informationsfreiheitsgesetzes des Bundes und ihrer Auswirkungen auf den Informationsanspruch der Antragstellerinnen und Antragsteller, BT-Drs. 16/2168

[166] Ein Jahr Informationsfreiheitsgesetz: Jahresbilanz 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

[167] Entschließung v. 26. Juni 2006: „Verbraucherinformationsgesetz nachbessern“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 124

[168] JB 2005, 4.9.4

Künftig können die vom öffentlichen Sektor bereitgehaltenen Informationen, die häufig wirtschaftlich gut verwertbar sind, auch von der Privatwirtschaft kommerziell genutzt werden. Zur Umsetzung der Europäischen Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors[169] hat der Bundestag das *Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen* (Informationsweiterverwendungsgesetz – IWG[170]) verabschiedet. Das Gesetz begründet kein eigenständiges Zugangsrecht zu Informationen, sondern knüpft an solche Informationen an, die öffentliche Einrichtungen bereits zur Verfügung stellen[171]. Die im Gesetzgebungsverfahren zutage getretenen Abgrenzungsschwierigkeiten zum Berliner Informationsfreiheitsgesetz, die vornehmlich dem unscharfen Begriff der „Weiterverwendung“ geschuldet waren[172], sind wohl durch die neue Definition beseitigt worden. Nunmehr ist „Weiterverwendung“ jede Nutzung von Informationen, die über die Erfüllung einer öffentlichen Aufgabe hinausgeht und in der Regel auf die Erzielung von Entgelt gerichtet ist; die intellektuelle Wahrnehmung einer Information und die Verwertung des dadurch erlangten Wissens stellen regelmäßig keine Weiterverwendung dar (so § 2 Nr. 3 IWG). Da das Berliner Informationsfreiheitsgesetz die kommerzielle Nutzung der Informationen nach § 13 Abs. 7 verbietet, scheint ein Konflikt mit dem IWG von vornherein nicht gegeben. Letztlich wird dies anhand konkreter Fälle zu überprüfen sein.

11.2 Weitere Entwicklungen für mehr *Transparenz*

Unter dem bezeichnenden Titel *Europäische Transparenzinitiative* hat die Europäische Kommission einen Vorstoß zu mehr Transparenz bei der Subventionsvergabe gewagt und hierzu eine öffentliche Konsultation initiiert[173]. Dazu gehört die Offenlegung von Informationen über Empfänger von EU-Geldern. Insbesondere im Bereich der Gemeinsamen Agrarpolitik variieren offenbar die von den Mitgliedstaaten jeweils zur Verfügung gestellten Informationen über die Begünstigten. Nach dem Willen der Europäischen Kommission sollen künftig Bürger im Internet nachlesen können, welche Firmen in welcher Höhe Subventionen erhalten haben. Nachdem der Bundeswirtschaftsminister dies zunächst nur für Fälle oberhalb eines Subventionswerts von 2 Millionen Euro zulassen wollte, gab die Bundesregierung letztlich den Widerstand gegen mehr Transparenz auf und verfolgte derartige „Subventionsschwellen“ nicht weiter. Sie tritt

[169] Richtlinie 2003/98/EG v. 17. November 2003

[170] v. 13. Dezember 2006, BGBl. I, 2913

[171] dazu bereits JB 2004, 4.9.2; JB 2005, 6.1

[172] JB 2005, 6.1

[173] Grünbuch der Kommission der Europäischen Gemeinschaften: Europäische Transparenzinitiative, KOM(2006) 194 endg.; Ratsdok. 9412/06, vgl. BR-Drs. 349/06

nun dafür ein, dass nicht jeder Mitgliedstaat der Europäischen Union die Daten veröffentlicht, sondern die Europäische Kommission selbst. Wir haben uns zusammen mit anderen Informationsfreiheitsbeauftragten an der öffentlichen Konsultation zur Europäischen Transparenzinitiative beteiligt und in einer Stellungnahme die Offenlegung von Informationen über Empfänger von EU-Geldern befürwortet. Die Ergebnisse der Konsultation mündeten in die EU-Haushaltsordnung für 2007–2013, die eine Offenlegung der Empfänger aller Subventionszahlungen vorsieht.

Auch innerhalb Deutschlands gleicht sich das Transparenzniveau weiter an. Landesinformationsfreiheitsgesetze sind nun auch in Bremen[174], Hamburg[175], Mecklenburg-Vorpommern[176] sowie im Saarland[177] in Kraft getreten. Mit Ausnahme des Hamburgischen Datenschutzbeauftragten haben alle Landesbeauftragten zugleich die Funktion des Informationsfreiheitsbeauftragten übernommen. Immerhin verfügt nun die Hälfte der Bundesländer über ein eigenes Informationsfreiheitsgesetz. Entsprechende Bemühungen der anderen Hälfte sind entweder im Keim erstickt (Baden-Württemberg, Bayern, Niedersachsen, Rheinland-Pfalz, Sachsen), mehr oder weniger Erfolg versprechend auf den parlamentarischen Weg gebracht (Sachsen-Anhalt, Thüringen) oder haben eine gewisse Aussicht auf Erfolg (Hessen).

11.3 Informationsfreiheit im Land Berlin

Mit dem *Achten Gesetz zur Änderung der Verfassung von Berlin (VvB)*[178] ist in einem neuen Artikel 45 Abs. 2 VvB das Recht der Abgeordneten auf Einsicht in Akten und sonstige amtliche Unterlagen der Verwaltung normiert worden. Die Einsichtnahme darf abgelehnt werden, soweit überwiegende öffentliche Interessen einschließlich des Kernbereichs exekutiver Eigenverantwortung oder überwiegende private Interessen an der Geheimhaltung dies zwingend erfordern. Nach der Gesetzesbegründung zählen hierzu insbesondere solche des Schutzes personenbezogener Daten und von Betriebs- und Geschäftsgeheimnissen. Die Neuregelung ist zu Beginn der 16. Wahlperiode des Abgeordnetenhauses, also mit Zusammentritt des neu gewählten Parlaments am 26. Oktober, in Kraft getreten. Zum Verfahren im Einzelnen bei Anträgen von Abgeordneten wurde eigens die *Gemeinsame Geschäftsordnung des Senats* (GGO I) um einen § 24 a erweitert[179].

[174] GVBl. v. 26. Mai 2006, 263
[175] GVBl. v. 21. April 2006, 167
[176] GVBl. v. 10. Juli 2006, 556
[177] ABl. v. 14. September 2006, 1624
[178] v. 25. Mai 2006, GVBl., 446
[179] GGO I v. 24. Oktober 2006

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Unseren Vorschlag, entsprechend der Rechtslage in Brandenburg ein Grundrecht auf Informationszugang in die Verfassung von Berlin aufzunehmen, hat das Abgeordnetenhaus nicht aufgegriffen. Dies sollte aber bei nächster Gelegenheit geschehen.

Mit dem *Dritten Gesetz zur Rechtsvereinfachung und Entbürokratisierung*[180] wurden zahlreiche Rechtsvorschriften aufgehoben und behördliche Verfahren vereinfacht mit dem Ziel des Bürokratieabbaus auch zugunsten des Bürgers. Groteskerweise hat dabei auch das IFG eine Änderung erfahren, die die *Transparenz* staatlichen Handelns zulasten des Bürgers begrenzt. Der neue § 9 beinhaltet einen nicht hinreichend bestimmten Ausnahmetatbestand, der für sich Anlass für gerichtliche Auseinandersetzungen bietet. Künftig soll der Informationszugang nicht erfolgen, wenn „nachteilige Auswirkungen für das Land Berlin bei der Durchführung eines laufenden Gerichtsverfahrens zu befürchten sind." Behörden könnten deshalb versucht sein, Ansprüche nach IFG bereits dann pauschal abzulehnen, wenn ein Prozess anhängig ist.[181] Deshalb raten wir dem Bürger, vor Beschreiten des (Zivil-) Rechtsweges gegen das Land Berlin zunächst die Rechte nach dem IFG auszuschöpfen. Eine weitere vom Senat angestrebte Änderung des IFG, mit der Informationen über fiskalische Tätigkeiten des Staates generell vom Anwendungsbereich des IFG ausgenommen werden sollten, scheiterte während der parlamentarischen Beratungen auch an unserem Widerstand.

Unser bereits seit Jahren geführte Kampf um eine bürgerfreundliche *Gebührenstaffel für Amtshandlungen nach IFG*[182] ist vielleicht schon bald beendet. Entweder soll die Gebührenregelung des Bundesumweltinformationsgesetzes in Landesrecht übernommen oder die mit der Senatsverwaltung für Inneres bereits erarbeitete Gebührenstaffel in die Verwaltungsgebührenordnung aufgenommen werden. Dies hat das Abgeordnetenhaus beschlossen[183].

Die Senatsverwaltung für Finanzen wird im ersten Halbjahr 2007 eine Änderungsverordnung zur Verwaltungsgebührenordnung vorlegen, worin eine Überarbeitung der Tarifstelle 1004 auf der Basis eines Änderungsvorschlages des Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie einer Empfehlung des Unterausschusses "Datenschutz und Informationsfreiheit" des Abgeordnetenhauses von Berlin aus der 15. Wahlperiode (vgl. Beschlussprotokoll der 38. Sitzung vom 15. März 2005) enthalten sein wird.

Bei der Neufassung der Tarifstelle mussten jedoch rechtswidrige Teile des Vorschlages unberücksichtigt bleiben. So sieht § 16 Berliner Informationsfreiheitsgesetz – IFG vor, dass die Akteneinsicht oder Aktenauskunft und das Widerspruchsverfahren gebührenpflichtig sind; ein vorgeschlagener Gebührenrahmen, der bei Null Euro beginnt, käme einer Gebührenbefreiung gleich und ist dementsprechend unzulässig. Zudem gilt, dass Abgabe begründende Tatbestände so bestimmt sein müssen, dass der Abgabepflichtige die

[180] v. 11. Juli 2006, GVBl., 819
[181] JB 2001, 4.9
[182] JB 2001, 4.9; JB 2004, 4.9.4; JB 2005, 6.2
[183] vgl. Anhang 1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

	auf ihn entfallende Abgabe vorausberechnen kann (z.B. BVerfG, 2 BvL 1/99 vom 17.07.2003). Bei einem bei Null Euro beginnenden Gebührenrahmen kann im voraus nicht abgeschätzt werden, ob die Auskunft faktisch gebührenfrei oder aber gebührenpflichtig ist. Auch wurden bspw. überflüssige Doppelregelungen nicht übernommen: Bei der Zurücknahme eines Antrages auf Akteneinsicht oder Aktenauskunft bevor die Behörde mit der Bearbeitung begonnen hat, wird bereits auf der Grundlage von § 6 Abs. 1 Satz 2 VGebO keine Gebühr erhoben.
Unsere mehr als siebenjährigen Erfahrungen als Schiedsstelle für IFG-Streitigkeiten zeigen im Übrigen, dass ein weiterer praktischer Schritt zu mehr Bürgerfreundlichkeit beim Umgang der Verwaltungen mit IFG-Anträgen sinnvoll ist. Zur besseren Handhabung nicht nur der Gebührenregelung, sondern auch der materiellen Voraussetzungen und einschränkenden Tatbestände des Informationszugangsanspruchs sollte in jeder Behörde ein Informationsfreiheitsbeauftragter „benannt“ werden. Diese Funktion könnte – entsprechend der Aufgabenkombination auf Landesebene – zugleich von dem behördlichen Datenschutzbeauftragten wahrgenommen werden. Insbesondere für große Verwaltungen wäre es von Vorteil, einen Informationsfreiheitsbeauftragten als Ansprechperson zu benennen. Durch eine zentrale Koordination würde ein Überblick über die Entscheidungspraxis der jeweiligen Verwaltung ermöglicht, sodass ggf. auf eine Vereinheitlichung hingewirkt werden kann. Daneben könnte der behördliche Informationsfreiheitsbeauftragte intern auch als Multiplikator für die Auffassungen der Informationsfreiheitsbeauftragten in Deutschland wirken. Die Bündelung der Erkenntnisse würde letztlich zu einer Verkürzung der Bearbeitungszeit zugunsten des Bürgers führen.	Der Senat teilt die Auffassung, dass die Benennung von Informationsfreiheitsbeauftragten sinnvoll sein kann, insbesondere in Behörden, die häufiger Anträge nach dem IFG zu bearbeiten haben. Dies sollte jedoch der Organisationshoheit der jeweiligen Behördenleitung überlassen bleiben.
11.3.1 Das Begehungsprotokoll und die Angst vor dem Schadensersatzanspruch *Eine Petentin beantragte durch ihren Rechtsanwalt beim Bezirksamt Friedrichshain-Kreuzberg die Herausgabe einer Kopie des Begehungsprotokolls über den Zustand eines Gehweges. Die Petentin hatte sich dort eine Fußverletzung zugezogen, die sie auf die Schadhaftigkeit des Gehweges zurückführte. Der Rechtsanwalt wollte zur Begründung des Schadenersatzanspruchs anhand des Begehungsprotokolls nachvollziehen, ob das Bezirksamt seiner Verkehrssicherungspflicht nachgekommen ist. Das Bezirksamt verweigerte den Informationszugang mit der Begründung, das IFG sehe eine derartige Verpflichtung in einer bevorstehenden zivilrechtlichen Streitigkeit, in der sich die Parteien auf der Ebene der Gleichrangigkeit gegenüberstehen, nicht vor. Die Protokolle würden aber im Falle eines Klageverfahrens dort vorgelegt werden. Nach eingelegtem Widerspruch hat uns der Rechtsanwalt um Unterstützung gebeten.*	

Wir haben dem Bezirksamt mitgeteilt, dass das IFG nicht danach unterscheidet, ob der Staat zivilrechtlich oder öffentlich-rechtlich handelt. Gerade im Vorfeld zivilrechtlicher Auseinandersetzungen ist ein Informationszugang unstreitig gegeben. Selbst wenn bereits ein Prozess anhängig gewesen wäre, hätte der Informationszugang zu dem bereits vor Klageerhebung vorhandenen Protokoll erfolgen müssen[184]. Dies muss erst recht gelten, wenn keine Klage anhängig ist, die womöglich durch Informationszugang vermieden werden kann. Nach einer Entscheidung des Verwaltungsgerichts Berlin[185] ist der Informationszugang weiter gehend für alle (d. h. auch noch nach Klageerhebung entstandenen) Unterlagen gegeben. Darüber hinaus geht das Gericht nicht von einer „echten“ Gleichrangigkeit bei Beteiligung des Staates aus. Das Bezirksamt ist unserer Auffassung gefolgt und hat die begehrten Kopien herausgegeben.

Auch bei zivilrechtlicher Tätigkeit des Staates ist das IFG anwendbar. Er darf Unterlagen nicht wegen einer befürchteten, aber noch nicht anhängigen Klage dem Informationszugang entziehen.

11.3.2 Die Stellungnahme an den *Petitionsausschuss* und der juristische Lapsus Spandaus

Eine Petentin hatte beim Petitionsausschuss des Abgeordnetenhauses eine Beschwerde im Zusammenhang mit dem vom Jugendamt Spandau wahrgenommenen Aufenthaltsbestimmungsrecht für ihre Kinder eingereicht. Entsprechend der üblichen Verfahrensweise hatte der Petitionsausschuss die Verwaltung um Stellungnahme gebeten, die der Bezirksbürgermeister Spandaus abgab. Da die Petition für die Bürgerin nicht erfolgreich war und sie die Hintergründe der Entscheidung des Petitionsausschusses nachvollziehen wollte, beantragte sie bei ihm die Herausgabe einer Kopie der Stellungnahme des Bezirksbürgermeisters. Der Petitionsausschuss lehnte dies unter Hinweis auf die ständige verwaltungsgerichtliche Rechtsprechung ab. Auf unsere Empfehlung wandte sich die Petentin an den Verfasser der Stellungnahme und bat dort um Herausgabe. Der Bezirksbürgermeister wies das Begehren der Petentin 2004 zurück. Hierüber informierte sie uns 2006 und bat erneut um Unterstützung.

Für den Informationszugang zu Unterlagen beim Petitionsausschuss des Abgeordnetenhauses gibt es weder im Petitionsgesetz noch im IFG noch im Berliner Datenschutzgesetz eine Anspruchsgrundlage. Da es sich bei dem Petitionsausschuss um ein parlamentarisches Kontrollorgan der Exekutive, mithin um einen Teil der Legislative handelt, ist das Berliner Daten-

[184] JB 2001, 4.9; möglicherweise andere Beurteilung nach dem neuen § 9 IFG, vgl. 11.3

[185] VG 23 A 93.03

schutzgesetz nicht anwendbar. Ebenso wenig gilt das IFG für die Prüfung und Bescheidung von Petitionen durch den Petitionsausschuss, der dabei keine Verwaltungsaufgabe erledigt (§ 2 Abs. 2 Satz 2 IFG). Zur Begründung seiner Auffassung, die Stellungnahme nicht ohne Einwilligung des Petitionsausschusses herauszugeben, bezog sich der Bezirksbürgermeister auf die Rechtsprechung des OVG Berlin[186]. Eine Herausgabe der eigenen Stellungnahme gegenüber dem Petitionsausschuss verstoße darüber hinaus direkt oder indirekt gegen § 10 Abs. 3 Nr. 2 IFG. Wir haben dem Bezirksbürgermeister mitgeteilt, dass der letzte Satz in dieser OVG-Entscheidung unsere Auffassung stützt: Die Antragstellerin habe „aufgrund des IFG umfassende Einsichts- und Auskunftsrechte gegenüber den betroffenen Behörden, mit dem ggf. erforderlich werdenden Rechtsschutz durch die Verwaltungsgerichte und notfalls auch durch den Verfassungsgerichtshof". Leider hat sich der Bezirksbürgermeister einer erneuten – von uns erbetenen „wohlwollenden" – Überprüfung seiner (bestandskräftigen) Ablehnung des Informationszugangsantrages verschlossen.

Bürger haben keinen Anspruch auf Informationszugang zu den Unterlagen beim Petitionsausschuss. Allerdings unterliegt die Stellungnahme der Verwaltung dem Informationszugang bei der Verwaltung selbst.

11.3.3 Bearbeitungsbitte durch das Bezirksamt Treptow-Köpenick

Ein Ehepaar hatte antragsgemäß beim Stadtplanungsamt Treptow-Köpenick Grundstücksakten eingesehen. Die beim Akteneinsichtstermin gestellte Frage, ob aus den Akten vor der Einsichtnahme Schriftstücke entnommen worden seien, wurde unter Hinweis auf die §§ 10, 11 IFG bejaht. Das Ehepaar bat daraufhin im Bezirksamt um Prüfung, ob diese Regelungen die Entnahme von Aktenteilen vor der Einsichtnahme rechtfertigten. Der Vorgang wurde uns vom Bezirksamt „zuständigkeitshalber" übersandt, da wir gemäß § 18 IFG für die Beantwortung der Fragen zuständig seien.

Wir haben dem Bezirksamt mitgeteilt, dass nach § 18 IFG unserer Behörde eine Schiedsstellenfunktion zukommt. Die Überprüfung eines Streitfalles durch uns – und ggf. die Schlichtung – kann nicht die primäre Pflicht des Bezirksamtes ersetzen, die Antragsteller ordnungsgemäß zu bescheiden. Das Bezirksamt hätte den Anspruch des Ehepaars auf einen schriftlichen (rechtsmittelfähigen) Bescheid erfüllen müssen. Denn es hat nicht alle in den Akten befindlichen Unterlagen zur Einsichtnahme vorgelegt und sich hierbei mündlich auf §§ 10,11 IFG berufen, ohne dies näher darzulegen.

[186] Beschluss v. 18. Oktober 2000 – OVG 2 M 15.00

Will ein Bürger wissen, aus welchem Grund die Akteneinsicht durch die öffentliche Stelle beschränkt worden ist, so hat diese – und nicht der Berliner Beauftragte für Datenschutz und Informationsfreiheit – ihn hierüber zu bescheiden.

11.3.4 Gebühren im Bezirksamt Treptow-Köpenick

Ein Petent begehrte im Tiefbauamt Treptow-Köpenick die Herausgabe einer Kopie eines zweiseitigen Gutachtens, das Vorschläge zu den in der Parchwitzer Straße durchzuführenden Arbeiten enthielt. Das Amt bewilligte die Akteneinsicht und nannte dafür einen Termin, zu dem der Einzahlungsbeleg als Nachweis für die zu entrichtende Verwaltungsgebühr vorzulegen sei. Die Gebühr belief sich auf 88,49 Euro. In seinem Widerspruch bat der Petent um Aufschlüsselung des Betrages. Das Bezirksamt reagierte darauf mit einem Fünfzeiler: „Der Antrag auf Akteneinsicht stellt keinen Verwaltungsakt dar, der ein Widerspruchsverfahren im Verwaltungssinn nach sich ziehen kann. Es ist jederzeit freigestellt, die Gebührenfestsetzung von einem Verwaltungsgericht prüfen zu lassen." Kurz darauf erhielt der Petent eine Mahnung.

Wir haben das Bezirksamt darauf hingewiesen, dass seine Auffassung unzutreffend ist. Wie sich aus § 14 IFG ergibt, ist die Versagung der Akteneinsicht im Widerspruchsverfahren überprüfbar. Dies gilt erst recht für die Kostenentscheidung. Auf unsere Initiative wurde die als prohibitiv empfundene Gebühr näher aufgeschlüsselt und schließlich um mehr als die Hälfte herabgesetzt. Leider ist dieser Fall ein weiteres Beispiel dafür, dass öffentliche Stellen den Bürger manchmal lieber in einen (auch für das Land Berlin Kosten verursachenden) Prozess treiben, anstatt seinen berechtigten IFG-Anspruch zu erfüllen.

Die für den Informationszugang erhobene Gebühr sollte für den Bürger nachvollziehbar berechnet sein und nicht erst im Prozess aufgeschlüsselt werden, der so vermieden werden kann.

11.3.5 TBC-Erkrankung im Wohnheim

Ein Petent verlangte von der Tuberkulose-Fürsorgestelle Mitte Hinweise zur Person eines in seinem Wohnheim für Obdachlose an TBC Erkrankten. Er wollte ausdrücklich nicht den Namen wissen, sondern nur, ob eine männliche oder eine weibliche Person betroffen war und aus welcher Wohngruppe die Person stammte. Der Petent hat vorgetragen, er wolle prüfen, ob er mit der erkrankten Person im Kontakt war bzw. künftigen Kontakt vermeiden muss. Die Fürsorgestelle hatte bereits mitgeteilt, dass es sich bei der Erkrankung um eine in der „untersten Stufe", also mit geringem Ansteckungsrisiko, gehandelt habe.

Wir haben das Informationszugangsbegehren nicht unterstützt. Zwar gestattet § 8 IFG unter bestimmten

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Voraussetzungen die Offenbarung von personenbezogenen Daten im Zusammenhang mit Angaben über Gesundheitsgefährdungen. Nach § 17 Abs. 4 IFG bleiben jedoch auf Bundesrecht beruhende Geheimhaltungspflichten unberührt. Das bedeutet, dass die dort geregelten Offenbarungsbefugnisse vorrangig zu berücksichtigen sind mit der Folge, dass § 8 IFG nicht gilt. Das Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten bei Menschen (Bundesinfektionsschutzgesetz) regelt in den §§ 6 ff. abschließend, in welchen Fällen welche Krankheiten namentlich oder nicht namentlich gegenüber welchen Stellen offenbart werden dürfen und müssen. Die Offenbarung von personenbezogenen oder möglicherweise personenbeziehbaren Angaben gegenüber Privatpersonen ist nicht vorgesehen und daher unzulässig. Darüber hinaus steht der Offenbarung der begehrten Angaben die *ärztliche Schweigepflicht* entgegen. Eine Verletzung dieser Geheimhaltungspflicht ist nach § 203 StGB strafbewehrt. Die Weitergabe der gewünschten Information an den Petenten wäre rechtswidrig gewesen.

Die Offenbarung personenbezogener Daten über Gesundheitsgefährdungen erlaubt keine Durchbrechung der ärztlichen Schweigepflicht.

11.3.6 Information über *Tierhalteverbot*

Eine Petentin hat vor dem Zivilgericht eine Klage auf Herausgabe von Katzen erhoben. Die Beklagte war der Auffassung, dass die Herausgabe der Tiere nicht beansprucht werden kann, weil die Petentin zur artgerechten Tierhaltung nicht in der Lage ist. Hierzu berief sich die Beklagte auf einen Bescheid des Veterinäramts Mitte, mit dem der klagenden Petentin die Tierhaltung untersagt worden war. Der Bescheid wurde der Beklagten auf ihren Antrag vom Bezirksamt in Kopie übersandt.

Nach §§ 3, 6 Abs. 1 und Abs. 2 Satz 1 Nr. 1 c) IFG durfte das Bezirksamt der Beklagten nur „Kerndaten“ wie den Namen und die Anschrift offenbaren sowie die *Tatsache* der gegenüber der Klägerin erfolgten „überwachenden oder vergleichbaren Verwaltungstätigkeit“, also die Tatsache der Untersagung der Tierhaltung. Die Herausgabe einer Kopie des vollständigen Bescheides, der auch detaillierte Informationen über die häuslichen Lebensumstände der Betroffenen enthielt, war unzulässig. Dabei war von uns nicht zu beurteilen, ob das Tierhalteverbot berechtigt ist. Die Akten hierzu hätten auf Anforderung des Gerichts an dieses übermittelt werden dürfen. Wir haben gegenüber dem Bezirksamt einen datenschutzrechtlichen Mangel festgestellt und den Fall zum Anlass genommen, die Bezirksämter in einem Rundschreiben über die Reichweite der Offenbarungsbefugnisse nach § 6 Abs. 2 IFG zu informieren.

Nach § 6 Abs. 2 IFG dürfen nur die dort genannten

personenbezogenen „Kerndaten“ offenbart werden sowie die *Tatsache* der Beteiligung des Betroffenen an einem Verfahren oder die *Tatsache* einer bestimmten rechtlichen Stellung des Betroffenen.

11.3.7 Auskunft über die Verfasser von Bildungsstandards

Ein Petent hat beim Sekretariat der Ständigen Konferenz der Kultusminister der Länder erfragen wollen, wer die Verfasser der Bildungsstandards im Fach Physik für den Mittleren Schulabschluss sind, insbesondere wer den Beschluss der Kultusministerkonferenz hierzu vorbereitet hat. Das Sekretariat verweigerte ihm die Auskunft unter Hinweis auf den Datenschutz.

Bei dem Sekretariat der Kultusministerkonferenz handelt es sich aufgrund eines Abkommens zwischen den Ländern um eine Dienststelle des Landes Berlin. Deshalb ist das IFG im Hinblick auf die dort vorhandenen Unterlagen anwendbar. Zu diesen Unterlagen gehören auch Listen mit den in den jeweiligen Kommissionen arbeitenden Mitgliedern aus den Bundesländern. Aus ser dem Ländervertreter Berlins unterfallen die Mitglieder nicht dem Anwendungsbereich des IFG, sodass das Sekretariat der Kultusministerkonferenz deren Zustimmung zur Offenbarung ihrer Daten erbeten hat (§ 10 Abs. 3 Nr. 2 BlnIFG). Einige sind dem gefolgt, sodass deren dienstliche Daten sowie diejenigen des Ländervertreters Berlin dem Petenten genannt wurden (§ 6 Abs. 2 Satz 1 Nr. 2 BlnIFG). Wegen der übrigen Kommissionsmitglieder haben wir dem Petenten empfohlen, in Ländern mit Informationsfreiheitsgesetzen die Informationsfreiheitsbeauftragten um Unterstützung zu bitten. Andernfalls sollten die Landesdatenschutzbeauftragten gefragt werden, ob der Auskunft über die Person der in der Kultusministerkonferenz agierenden Ländervertreter tatsächlich Datenschutzgründe entgegenstehen. Diese Frage hätten wir unter Hinweis auf § 6 Abs. 1 Satz 2 BlnDSG verneint.

Personenbezogene (dienstliche) Daten Berliner Amtsträger, die in gemischten Ländergremien agieren, sind in der Regel zu offenbaren.

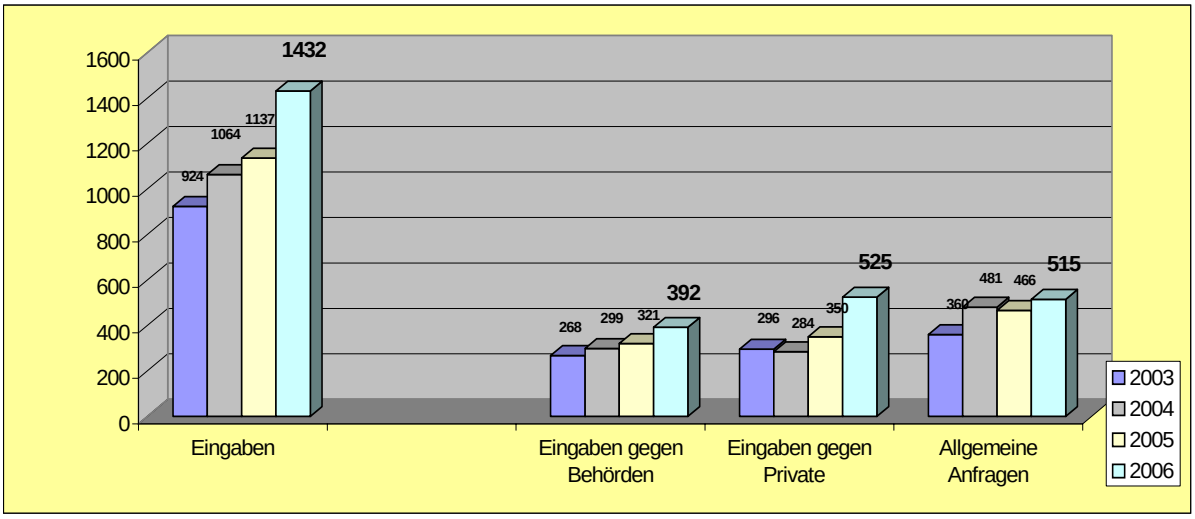
12 Entwicklung

Die zunehmenden Überwachungstendenzen in Staat und Gesellschaft führen dazu, dass auch die Anforderungen an die Dienststelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit zunehmen. Dies lässt sich u. a. daran ablesen, dass die Eingaben von Bürgerinnen und Bürgern zwischen 2003 und 2006 um rund 50 % gestiegen sind[187]. Besonders stark

[187] vgl. Abbildung

ist die Zahl der Eingaben gegen Datenverarbeiter im nicht-öffentlichen Bereich (in erster Linie Wirtschaftsunternehmen) gestiegen. Diese Zahlen machen deutlich, dass – ganz im Gegensatz zu manchen öffentlichen Behauptungen – der Datenschutz nicht an Bedeutung verliert, sondern sich immer mehr Menschen gegen eine verstärkte Beobachtung und Registrierung wenden. Die Dienststelle setzt alles daran, diesen Beschwerden möglichst zeitnah nachzugehen. Sie muss allerdings außerdem neue IT-Verfahren begleiten und kontrollieren und zudem in zahlreichen Gesetzgebungsverfahren auf Landes- und Bundesebene Gesichtspunkte des Datenschutzes und der Informationsfreiheit zur Geltung bringen.

Entwicklung der Anzahl von schriftlichen (einschließlich E-Mail) Eingaben an den Berliner Beauftragten für Datenschutz und Informationsfreiheit in den Jahren 2003 bis 2006



12.1 Zusammenarbeit mit dem Abgeordnetenhaus

Im zurückliegenden Jahr hat der Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses die Beratung der Stellungnahme des Senats zum Jahresbericht 2004 abgeschlossen und außerdem zahlreiche aktuelle Fragen des Datenschutzes und der Informationsfreiheit erörtert. Die Diskussionen im Unterausschuss zeigen immer wieder, dass Fragen des Datenschutzes und der Informationsfreiheit erfreulicherweise nicht zum Gegenstand parteipolitischer Auseinandersetzungen gemacht werden. Vielmehr hat der Unterausschuss mehrfach einmütig Empfehlungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit aufgegriffen und den Senat zu entsprechenden Maßnahmen aufgefordert. Die Entschlies sungen des Unterausschusses zum Jahresbericht 2004 wurden vom Abgeordnetenhaus in der Sitzung am 31.

August 2006[188] beschlossen.

12.2 Zusammenarbeit mit anderen Stellen

Nur eine vernetzte Datenschutzkontrolle auf nationaler und internationaler Ebene hat die Chance, Risiken für den Datenschutz und die Transparenz rechtzeitig zu erkennen und gemeinsame Konzepte für ihre Beherrschung zu entwickeln.

Das wichtigste Koordinierungsgremium auf nationaler Ebene im öffentlichen Bereich ist die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, die im Berichtszeitraum unter dem Vorsitz des Landesbeauftragten für den Datenschutz Sachsen-Anhalt am 16./17. März 2006 in Magdeburg und am 26./27. Oktober 2006 in Naumburg getagt hat. Sie hat in und zwischen diesen Sitzungen mehrere Entschließungen zu aktuellen Themen des Datenschutzes gefasst, die auch für die Bundeshauptstadt von Bedeutung sind[189]. 2007 übernimmt der Thüringer Landesbeauftragte für Datenschutz den Vorsitz der Konferenz.

Gemeinsam mit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg haben wir einen „Ratgeber zu Hartz IV“ herausgegeben, in dem konkrete Hinweise zu Datenschutzfragen beim Bezug von Arbeitslosengeld II gegeben werden. Dieser Ratgeber wird außerordentlich stark nachgefragt, was deutlich macht, welch hoher Beratungsbedarf in diesem für viele Menschen existenziell wichtigen Bereich besteht. Dies bestätigt auch die anhaltend hohe Zahl von Anfragen und Beschwerden in beiden Dienststellen. Der „Ratgeber Hartz IV“ ist nur ein Beispiel für die enge und gute Zusammenarbeit zwischen den Dienstellen in Brandenburg und Berlin[190].

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich trafen sich im *„Düsseldorfer Kreis“* unter dem Vorsitz des Landesbeauftragten für den Datenschutz Freie Hansestadt Bremen am 26./27. April und 8./9. November 2006. In der zuletzt genanten Sitzung fasste der Düsseldorfer Kreis erstmals zwei auch für die Öffentlichkeit gedachte Beschlüsse zum *SWIFT*-Verfahren und zur Entwicklung und Anwendung der *RFID-Technologie*[191]. Im Jahr 2007 führt der Hamburgische Datenschutzbeauftragte turnusmäßig den Vorsitz im Düsseldorfer Kreis. Weiterhin betreuen wir die Arbeitsgruppen „Internationaler Datenverkehr[192]“ und „Telekommunikation, Tele- und Mediendienste“ dieses Kreises.

---

188 vgl. Anhang 1

189 vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 9 ff.

190 Außerdem wurden gemeinsame Faltblätter zur *RFID-Technologie* und zu Biometrischen Verfahren entwickelt.

191 vgl. Anlagenband, a.a.O., S. 21

192 vgl. dazu 8.3

Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland hat im Berichtszeitraum durch die Verabschiedung weiterer Informationsfreiheitsgesetze in den Ländern drei weitere Mitglieder aus Bremen, Mecklenburg-Vorpommern und dem Saarland erhalten. Sie tagte im vergangenen Jahr am 26. Juni und 12. Dezember unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Bonn und fasste mehrere Entschließungen zur Verwaltungstransparenz und zum Verbraucherinformationsgesetz[193]. Im ersten Halbjahr 2007 wird der Leiter des Unabhängigen Landeszentrums Schleswig-Holstein den Vorsitz der Arbeitsgemeinschaft, die sich künftig „Konferenz der Informationsfreiheitsbeauftragten“ nennt, übernehmen.

Die Interessen der Aufsichtsbehörden der Bundesländer auf europäischer Ebene vertritt der Berliner Beauftragte für Datenschutz und Informationsfreiheit in der *Arbeitsgruppe nach Art. 29* der Europäischen Datenschutzrichtlinie, die zahlreiche, zum Teil umfangreiche Stellungnahmen zu europaweit bedeutsamen Fragen des Datenschutzes verabschiedete[194]. Bei zwei von der Europäischen Kommission im Oktober 2006 veranstalteten Konferenzen zur RFID-Technologie und zum grenzüberschreitenden Datenverkehr erläuterte der Berliner Datenschutzbeauftragte die Position der europäischen Aufsichtsbehörden. Am 24./25. April 2006 fand in Budapest die *Europäische Datenschutzkonferenz* auf Einladung des Ungarischen Beauftragten für Datenschutz und Informationsfreiheit statt[195]. Bei der *Internationalen Konferenz der Datenschutzbeauftragten* am 3. November 2006 in London wurde u. a. eine von ihm vorgeschlagene Entschließung zum Datenschutz bei Suchmaschinen beschlossen[196].

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) tagte unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 6./7. April 2006 in Washington D. C. und am 5./6. September 2006 im Anschluss an das Internationale Symposium im Rahmen der Funkausstellung[197] in Berlin. Die Arbeitsgruppe beschloss Stellungnahmen zu so unterschiedlichen Themen wie der elektronischen Gesundheitsakte, der Internet-Telefonie und Technologien zur digitalen Rechteverwaltung; außerdem wurde ein Arbeitspapier zu Suchmaschinen aktualisiert[198]. Am 25.

[193] vgl. Anlagenband, a.a.O., S. 124 ff.
[194] vgl. Anlagenband, a.a.O., S. 30 ff.
[195] vgl. Anlagenband, a.a.O., S. 27 ff.
[196] vgl. 10.2.3 und Anlagenband, a.a.O., S. 93
[197] vgl. 10.4
[198] vgl. Anlagenband, a.a.O., S. 112

September 2006 nahm der Berliner Beauftragte für Datenschutz und Informationsfreiheit bei einer Sitzung des Governmental Advisory Committee (GAC), einem Beratungsgremium für die Internet-Dachorganisation ICANN, Stellung zu Datenschutzfragen im Zusammenhang mit der WHOIS-Datenbank.

Auf Einladung der katalanischen Datenschutzbehörde tagte am 4./5. Oktober 2006 die *1. Konferenz der Datenschutzbeauftragten in Föderalstaaten* in Barcelona. Bei dieser Gelegenheit erläuterte der Berliner Beauftragte für Datenschutz und Informationsfreiheit das erfolgreiche Modell der Bund-Länder-Kooperation unter den Aufsichtsbehörden in Deutschland.

Die *Internationale Konferenz der Informationsfreiheitsbeauftragten* fand am 22./23. Mai 2006 unter dem Vorsitz des britischen Information Commissioner in Manchester statt.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat sich im Rahmen einer Anhörung im Innenausschuss des Sächsischen Landtages zur inzwischen in Kraft getretenen Änderung des Sächsischen Datenschutzgesetzes geäußert, mit der die Kontrollkompetenz für den Datenschutz im nicht-öffentlichen Bereich auf den Sächsischen Datenschutzbeauftragten übertragen worden ist.

12.3 Europäische Akademie für Informationsfreiheit und Datenschutz

Die *Europäische Akademie für Informationsfreiheit und Datenschutz* hat im Berichtszeitraum mit unserer Unterstützung zwei Veranstaltungen durchgeführt. Ein Workshop zur elektronischen Verfolgung von Fahrzeugen (Vehicle Event Recording) fand am 28. März 2006 statt und am 14. September 2006 beschäftigte sich ein weiterer Workshop mit dem Thema „Serverbasierte Datenverarbeitung und Datenschutz[199]“.

12.4 Öffentlichkeitsarbeit

Um die Öffentlichkeit auch persönlich über unsere Tätigkeit zu informieren, haben wir uns im Berichtszeitraum wieder an mehreren öffentlichen Veranstaltungen beteiligt:

- Berliner Verbraucherfest am 22. April 2006
- Tag der offenen Tür des Abgeordnetenhauses von Berlin am 13. Mai 2006
- 35. Tag der offenen Tür der Berliner Polizei am 9. September 2006.

Die Resonanz bei den Bürgerinnen und Bürgern war

[199] vgl. 2.5

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

jeweils groß. Wir haben zu diesem Zweck ein neues Faltblatt entwickelt, in dem unsere Aufgaben und Möglichkeiten zusammengefasst werden. Dieses Faltblatt ist mittlerweile auch in türkischer Sprache erhältlich.

Berlin, den 28. März 2007

Dr. Alexander Dix

Berliner Beauftragter für Datenschutz
und Informationsfreiheit