Jahresbericht 2005

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2005

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den ***am 15. März 2005*** *vorgelegten Jahresbericht 2004 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2005 ab.*

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Anlagenband („Dokumente zu Datenschutz und Informationsfreiheit 2005“) veröffentlicht, der gemeinsam mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg herausgegeben wird.

*Dieser Jahresbericht ist über das Internet (*http://www.datenschutz-berlin.de/*) abrufbar.*

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4 – 10, 10787 Berlin
Telefon: (0 30) + 138 89-0
Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de/

Redaktion: Laima Nicolaus

Druck: Brandenburgische Universitätsdruckerei
und Verlagsgesellschaft Potsdam mbH

Inhaltsverzeichnis

1. Entwicklung des Datenschutzrechts.....11
1.1 Europa.....11
1.2 Deutschland.....14
1.3 Berlin.....16
2. Technische Rahmenbedingungen.....18
2.1 Entwicklung der Informationstechnik.....18
2.2 Datenverarbeitung in der Berliner Verwaltung.....27
3. Schwerpunkte im Berichtsjahr.....37
3.1 Videoüberwachung in öffentlichen Verkehrsmitteln und Wohnanlagen 37
Kameras in Wohnanlagen – die kostenlose Live-Fernsehshow.....42
3.2 Hartz IV und kein Ende.....44
3.3 „Rasterfahndung“ zur Bekämpfung der Geldwäsche 50
3.4 Immer wichtiger: Anonymisierung und Pseudonymisierung.....55
3.5 Wie ist SPAM zu bekämpfen?.....60
3.6 Prüfung eines der größten Datenverarbeiter in Deutschland – der GEZ 65
4. Aus den Arbeitsgebieten.....72
4.1 Öffentliche Sicherheit.....72
4.1.1 Polizei.....72
4.1.2 Verfassungsschutz.....84
4.2 Ordnungsverwaltung.....89
4.2.1 Melde-, Personenstands- und Ausländerwesen 89
4.2.2 Verkehr 97
4.3 Justiz 99
Zweckentfremdung von Halterdaten.....110
4.4 Finanzen.....111
4.5 Sozialordnung.....115
4.5.1 Gesundheit.....115
4.5.2 Sozial- und Jugendverwaltung.....128
4.5.3 Personaldatenschutz.....131
4.5.4 Wohnen.....135
4.6 Wissen und Bildung.....137
4.6.1 Wissenschaft und Forschung.....137
4.6.2 Statistik.....145
4.6.3 Schule.....149
4.7 Wirtschaft.....158
4.7.1 Verkehrsunternehmen 158
4.7.2 Banken und Auskunfteien.....164
4.7.3 Was wir sonst noch geprüft haben 169
4.8. Europäischer und internationaler Datenschutz.....178
4.8.1 Europäische Union.....178
4.8.2 Der datenschutzgerechte Schutz von „Whistleblowern“.....180
4.8.3 Datenübermittlung an die Auslandshandelskammern (AHKs)183
4.9 Organisation und Technik.....184
4.9.1 Behördliche Datenschutzbeauftragte.....184

4.9.2 Kontrolle des Verfahrens SpDI32 192
4.9.3 Datenschutz im IT-Verfahren IPV.....195
4.9.4 Sicherheit in lokalen Funknetzen (WLAN).....196
4.9.5 Datensicherheit bei digitalen Kopiersystemen.....197
5. Telekommunikation und Medien.....200
5.1 Telekommunikationsdienste.....200
5.2 Teledienste.....205
5.3 Medien.....213
6. Informationsfreiheit 214
6.1. Informationsfreiheit auf Bundesebene.....214
6.2 Informationsfreiheit im Land Berlin.....217
Akteneinsicht bei Botschaftsgrundstücken?.....222
7. Aus der Dienststelle 224
7.1 Entwicklung.....224
7.2 BürgerOffice.....224
7.3 Zusammenarbeit mit dem Abgeordnetenhaus.....225
7.4 Zusammenarbeit mit anderen Stellen.....225
7.5 Europäische Akademie für Informationsfreiheit und Datenschutz...227
7.6 Öffentlichkeitsarbeit.....228

Anhang

1. Beschlüsse des Abgeordnetenhauses
2. Hinweise zur SPAM-Bekämpfung
3. Auszug aus dem Geschäftsverteilungsplan des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Stichwortverzeichnis

Einleitung

In den Berichtszeitraum fiel der Wechsel im Amt des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Mit meiner Wahl durch das Abgeordnetenhaus von Berlin endete die Amtszeit von Herrn Prof. Dr. Dr. Hansjürgen Garstka, der dieses Amt (zunächst das des Berliner Datenschutzbeauftragten) insgesamt 15 Jahre lang ausgeübt hat. Zuvor war er seit der Gründung der Dienststelle des Berliner Datenschutzbeauftragten 1979 als dessen Vertreter tätig, so dass er insgesamt fast 26 Jahre lang die Gestaltung und Kontrolle des Datenschutzes und seit dem Jahr 2000 auch die Durchsetzung der Informationsfreiheit in Berlin maßgeblich geprägt hat. Sein Verdienst ist es, dass Berlin nicht nur bundesweit, sondern auch europa- und weltweit in Fragen des Datenschutzes und der Informationsfreiheit einen exzellenten Namen hat. Dafür sei ihm auch an dieser Stelle herzlich gedankt. Er hat die Dienststelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu einem bürgerorientierten Kompetenzzentrum gemacht. Erfreulicherweise bleibt Herr Prof. Garstka Berlin in seiner Eigenschaft als Vorstandsvorsitzender der *Europäischen Akademie für Informationsfreiheit und Datenschutz* erhalten. Wir werden die von Anfang an enge Zusammenarbeit mit der Europäischen Akademie fortsetzen.

Die Herausforderungen, denen sich der Datenschutz angesichts einer rasanten technologischen Entwicklung und neuer Bedrohungen gegenüber sieht, haben sich im zurückliegenden Jahr weiter erhöht. Dabei kann kein Zweifel daran bestehen, dass – wie es die Datenschutzbeauftragten des Bundes und der Länder im Oktober 2005 formuliert haben[1] – eine moderne Informationsgesellschaft *mehr* Datenschutz braucht. Das Vertrauen der Bürgerinnen und Bürger gegenüber der Verwaltung wie auch der Wirtschaft ist untrennbar verbunden mit verstärkten Vorkehrungen gegen permanente Registrierung und Beobachtung. Der Richter am Bundesverfassungsgericht Prof. Dr. Wolfgang Hoffmann-Riem hat darauf hingewiesen, dass ein Staat, der seinen Bürgerinnen und Bürgern mit generellem Misstrauen begegnet, darauf gefasst sein muss, dass diese umgekehrt dem Staat zunehmend misstrauen. Entsprechendes trifft zu für die Wirtschaft, zumal sich der Staat ihrer zunehmend bedient, um bürgerbezogene Informationen auf Vorrat für künftige Zwecke zu sammeln. In diesem Zusammenhang und vor dem Hintergrund der Diskussionen im zurückliegenden Jahr sind mehrere Klarstellungen zur Bedeutung des Grundrechts auf Datenschutz nötig:

Zum einen: Das in der Verfassung von Berlin[2] garantierte Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, schützt

1 Entschließung der 70. Konferenz, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 21

2 Art. 33

mehr als die Privat- oder Intimsphäre. Das Recht auf informationelle Selbstbestimmung beschränkt sich nicht auf einen *Kernbereich der persönlichen Lebensgestaltung*, sondern betrifft alle, auch die öffentlichen Lebenszusammenhänge. Diese Klarstellung ist deshalb wichtig, weil bei der heftigen öffentlichen Diskussion, die gegenwärtig über die *Videoüberwachung* im öffentlichen Verkehrsnetz geführt wird, häufig von den Befürwortern verstärkter Videoaufzeichnung die These vertreten wird, niemand könne sich im öffentlichen Raum auf den Schutz seiner Privatsphäre berufen. Dieser Einwand geht deshalb fehl, weil das Grundrecht auf Datenschutz einen weitergehenden Anwendungsbereich hat als etwa das Grundrecht auf Unverletzlichkeit der Wohnung.

Es ist zwar richtig, dass das Bundesverfassungsgericht in seiner Entscheidung zum Großen Lauschangriff[3] den Kernbereich privater Lebensgestaltung grundsätzlich von allen Maßnahmen der staatlichen Überwachung freigestellt hat. Diese Entscheidung darf aber nicht dahingehend missverstanden werden, dass auch der Datenschutz auf den Schutz der *Intimsphäre* oder des Kernbereichs der persönlichen Lebensgestaltung reduziert wird. Informationelle Selbstbestimmung ist eine Grundvoraussetzung für die freie Kommunikation und Interaktion einer freien Gesellschaft. Sie umfasst deshalb auch das Recht aller, sich im öffentlichen Raum bewegen zu können, ohne dass die eigenen Verhaltensweisen rund um die Uhr von Videokameras beobachtet und aufgezeichnet werden. Natürlich gibt es Ausnahmen von diesem Grundsatz, aber deren Umfang muss sorgfältig abgewogen werden. Es geht nicht an, eine Rundumüberwachung aller Bewegungen von Menschen im öffentlichen Raum damit zu rechtfertigen, dass sie sich aus ihrer Privatsphäre hinausbegeben hätten. Das Grundrecht auf Datenschutz gilt auch im öffentlichen Raum und kann nur im überwiegenden Allgemeininteresse im Rahmen der Verhältnismäßigkeit aufgrund eines Gesetzes eingeschränkt werden.

Eine weitere verkürzte Vorstellung vom Datenschutz, die in jüngster Zeit um sich greift, besteht in der unzutreffenden These, der Datenschutz werde nur bei einem Missbrauch personenbezogener Daten verletzt. Zwar ging noch das erste Bundesdatenschutzgesetz von 1978 von dem Ziel aus, Missbrauch im Umgang mit personenbezogenen Daten verhindern zu wollen. Diese Vorstellung vom Datenschutz, die sich auf die Sicherung vorhandener Datenbestände beschränkt, ist jedoch mittlerweile überholt. Die Datenschutzgesetze des Bundes und der Länder unterwerfen schon die Erhebung personenbezogener Daten strikten rechtlichen Beschränkungen, weil bereits darin ein Grundrechtseingriff liegt. Eingriffe in Grundrechte sind jedoch stets die rechtfertigungsbedürftige Ausnahme, sie dürfen nicht zur Regel werden. Daran ist gerade angesichts einer zunehmenden Tendenz zur *Vorratsdatenspeicherung* zu erinnern, die häufig mit dem Argument verteidigt wird, gegen eine unbegrenzte Sammlung personenbezogener Daten spreche so lange nichts, wie ihre anschließende zweckgebundene Verwendung

3 v. 3. März 2005, vgl. dazu JB 2004

und Sicherung gegen Missbrauch gewährleistet werde.

Auch die Diskussion über die Nutzung von Daten zur Erhebung der Autobahnmaut im vergangenen Jahr hat gezeigt, dass nicht einmal die vom Gesetzgeber ausdrücklich beschlossene Zweckbindung mit einem nachträglich ergänzten Verwertungsverbot für andere Zwecke verhindern kann, dass die *Mautdaten* später einer anderen Verwendung (hier: der Aufklärung von Straftaten) zugeführt werden, wenn eine politische Mehrheit dies für zweckmäßig hält. Es ist mit Recht darauf hingewiesen worden, dass das Autobahnmautgesetz seinerzeit ohne die strikte Zweckbindung der erhobenen Daten „nicht verabschiedet worden wäre“[4]. Hieran wird überdeutlich, dass jede Einführung neuer Datenverarbeitungsverfahren, die mit Erhebung personenbezogener Daten einhergehen, datenschutzrechtliche Risiken auslöst. Es genügt nicht mehr, sich auf eine einmal gegebene Zusage des Gesetzgebers zu verlassen, dass personenbezogene Daten nicht zweckentfremdet werden dürfen. Derartige gesetzliche Festlegungen können bei geänderten politischen Mehrheiten ohne weiteres revidiert werden, soweit der verfassungsrechtliche Rahmen dies zulässt. Auch wenn die Verwendung von Mautdaten für Zwecke der Verfolgung schwerer Straftaten nicht gegen die Würde des Menschen verstößt[5], so wären durch einen solchen Schritt Festlegungen des Gesetzgebers über die ursprüngliche Zweckbindung erhobener Daten generell in Frage gestellt. Jetzt rächt es sich zudem, dass bei der Einführung der *Autobahnmaut* ein Verfahren gewählt würde, das das Prinzip der Datenvermeidung nicht berücksichtigt, sondern technisch ein erhebliches Überwachungspotenzial für beliebige Zwecke bürgt.

Wer sich in den Forschungslaboren der Industrie informiert, wird erkennen, dass die Bedeutung sog. *Metadaten* (Informationen über andere – inhaltliche – Informationen, z. B. wer hat mit wem wie lange von wo aus telefoniert) immer mehr zunimmt. Neben den Verkehrsdaten in der Telefon- und Internetkommunikation sind dies z. B. auch die Daten, die jede Digitalkamera heute über die gemachten Aufnahmen speichert und uns der Mühe enthebt, sich an die Umstände jedes einzelnen Schnappschusses zu erinnern. Diese Metadaten haben einen eigenen Informationsgehalt, der vieles über die Lebens- und Reisegewohnheiten von Menschen aussagt und jederzeit zu einem Persönlichkeitsprofil des Urhebers zusammengefasst werden kann. Es ist ein folgenschwerer Irrtum zu meinen, die bloße Erhebung solcher Daten auf Vorrat sei unkritisch und führe nicht zu einer Einschränkung der informationellen Selbstbestimmung. In einer Welt der allgegenwärtigen Rechentechnik (des *„ubiquitous computing“*) können RFID-Chips oder Sensoren die Bewegungen von Personen noch besser registrieren als Video-kameras. Die informationelle Selbstbestimmung lässt sich deshalb nur dann aufrechterhalten, wenn schon die Erhebung personenbezogener Daten auf das zwingend notwendige Minimum beschränkt wird. In einer modernen Informationsgesellschaft sind Datenvermeidung und

4 so der Vorsitzende der CSU-Fraktion am Bayerischen Landtag, Abg. Herrmann
5 so Generalbundesanwalt Nehm beim Verkehrsgerichtstag 2006

Datensparsamkeit Grundvoraussetzungen für die Autonomie des Einzelnen.

1. Entwicklung des Datenschutzrechts

1.1 Europa

Das Europäische Parlament hat am 14. Dezember 2005 dem Vorschlag für eine Richtlinie über die *Vorratsspeicherung* von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, zugestimmt. Auch wenn diese Richtlinie zum Ende des Berichtszeitraums noch nicht endgültig vom Rat beschlossen worden war, bahnt sich damit ein Dammbruch zu Lasten des Datenschutzes in Europa an[6]. Die Mitgliedstaaten wären danach gehalten, Anbieter elektronischer Kommunikationsdienste zur pauschalen und anlassunabhängigen Speicherung sämtlicher bei der Nutzung dieser Dienste anfallender Verkehrsdaten für einen Zeitraum von sechs Monaten bis zu zwei Jahren zu verpflichten. Die Datenschutzbeauftragten in Europa und Deutschland haben dieses Vorhaben bis zuletzt grundsätzlich abgelehnt, weil dadurch das in der *Europäischen Menschenrechtskonvention* garantierte Recht auf freie und unbeobachtete Kommunikation verletzt wird[7].

Es ist schwer vorstellbar, dass eine solche Richtlinie, sollte sie In-Kraft-treten, in Deutschland ohne Verstoß gegen die Verfassung umgesetzt werden kann. In jedem Fall wird es darum gehen, dass der deutsche Gesetzgeber die verbleibenden Spielräume der europäischen Rahmenregelung etwa hinsichtlich des Speicherungszeitraumes und der Verwendungszwecke der gespeicherten Verkehrsdaten so restriktiv und so grundrechtsschonend wie möglich nutzt. Dies hat das Bundesverfassungsgericht bereits in seiner Entscheidung zum Europäischen Haftbefehl betont[8].

Welche Auswirkungen eine verdachtsunabhängige *Vorratsdatenspeicherung* (die erst der Verdachtsgewinnung dienen soll) haben wird, zeigt sich gegenwärtig in den Vereinigten Staaten von Amerika. Dort hat die Justiz die großen Betreiber von Suchmaschinen zur Offenlegung bestimmter Suchanfragen und Internetadressen aufgefordert, um auf dieser Grundlage strafbaren Inhalten im Internet nachgehen zu können. Nur zum Teil haben sich die Suchmaschinenbetreiber dem Ansinnen widersetzt. Anders als in Deutschland sind sie allerdings nicht zur Löschung von Nutzungsdaten nach dem Ende der Verbindung verpflichtet, sondern speichern derartige Suchanfragen teilweise unbegrenzt. Wenn man sich vergegenwärtigt, dass die gesuchten Begriffe und Fragen, die wir in eine *Suchmaschine* eingeben, unsere Gedanken und Vorlieben widerspiegeln und mit den Worten eines

---

6 vgl. 5.

7 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Stellungnahme der Art. 29-Datenschutzgruppe, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 14, 31

8 Urteil v. 18. Juli 2005 – 2 BvR 2236/04 – http://www.bverfg.de/entscheidungen/rs20050718_2bvr223604.html

amerikanischen Bürgerrechtlers einem „Ausdruck unseres Gehirns“ gleichkommen, wird die Tragweite der Nutzbarkeit dieser Daten durch Dritte für welche Zwecke auch immer deutlich. Wohl gemerkt: Das Stellen von Fragen ist weder online noch offline mit Strafe bedroht, weder in den USA noch in Deutschland.

Auch eine zweite Entwicklung in den USA stimmt nachdenklich: In mehreren Fällen sind dort gespeicherte Telefon-Verbindungsdaten im großen Stil – z. B. im Internet – zum Verkauf angeboten worden. Darunter befanden sich auch Informationen darüber, von welchen Patienten ein Arzt angerufen wurde. Dieses Beispiel macht deutlich, dass vorhandene Datenbestände, die bei einer verpflichtenden Vorratsdatenspeicherung noch drastisch anwachsen würden, sich nicht zuverlässig vor dem Zugriff Dritter, seien es staatliche Behörden oder private Interessenten, schützen lassen. Entscheidend aber bleibt, dass bei der Einführung der obligatorischen Vorratsdatenspeicherung jeder, der elektronische Kommunikationsnetze nutzt, unter *Generalverdacht* gestellt wird. Sollten die Daten auch dann gespeichert bleiben, wenn der Kunde seine Telefon- oder Internetrechnung längst bezahlt hat, kann von einer freien, unbeobachteten Kommunikation keine Rede mehr sein.

Im Juli 2005 leitete die Europäische Kommission ein *Vertragsverletzungsverfahren* gegen die Bundesrepublik ein, weil sie die Auffassung vertritt, dass die Stellung der Aufsichtsbehörden für den nicht-öffentlichen Bereich in allen 16 Ländern der Bundesrepublik Deutschland gegen Art. 28 der Datenschutzrichtlinie 95/46/EG verstößt. Darin wird eine „völlige *Unabhängigkeit*“ dieser Aufsichtsbehörden europaweit vorgeschrieben. Auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat seit jeher die Auffassung vertreten, dass jedenfalls den Aufsichtsbehörden in solchen Ländern die völlige Unabhängigkeit fehlt, in denen sie Teil der Ministerialverwaltung sind. Die Europäische Kommission sieht aber auch in der in Berlin vorgesehenen Rechts- und Dienstaufsicht über den Berliner Beauftragten für Datenschutz und Informationsfreiheit eine Beschränkung der völligen Unabhängigkeit, die mit der Richtlinie nicht vereinbar sei. Die Bundesregierung hat in ihrer Stellungnahme gegenüber der Kommission ihren alten Standpunkt bekräftigt, wonach das System der Datenschutzkontrolle gerade im nicht-öffentlichen Bereich durch die Datenschutzrichtlinie nicht verändert werden sollte. Neue Gesichtspunkte hat die Bundesregierung in diesem Zusammenhang nicht vorgebracht. Es ist deshalb davon auszugehen, dass die Europäische Kommission den Europäischen Gerichtshof anrufen wird, dessen Entscheidung weitreichende Konsequenzen für die Struktur der *Datenschutzaufsicht* in Deutschland haben wird.

Am 6. Oktober 2005 hat die Kommission zwei Vorschläge für Rahmenbeschlüsse vorgelegt, die den Datenschutz im Rahmen der polizeilichen und justiziellen Zusammenarbeit (der sog. dritten Säule) auf eine neue Grundlage stellen sollen. Der Vorschlag für einen Rahmenbeschluss des

Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[9], erstreckt die Grundsätze, die in der allgemeinen Datenschutzrichtlinie von 1995 für den Binnenmarkt europaweit formuliert worden sind, auf den Bereich der Zusammenarbeit von Polizei und Strafverfolgungsbehörden in der Europäischen Union. Zu dem weiteren Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit[10] ist vorgesehen, dass Strafverfolgungsbehörden und Bedienstete von *EUROPOL* direkten Onlinezugang zu verfügbaren Informationen oder zu offline vorhandenen Indexdaten erhalten sollen. Die beiden geplanten Rahmenbeschlüsse stehen in einem engen Zusammenhang und zugleich in einem erheblichen Spannungsverhältnis. Denn der formulierte „*Grundsatz der Verfügbarkeit*“ widerspricht diametral den datenschutzrechtlichen Prinzipien der Erforderlichkeit, Zweckbindung und Datensparsamkeit. Die Beratungen für beide Vorschläge der Kommission wurden im Berichtszeitraum nicht mehr abgeschlossen.

Bereits im Mai 2005 hatte die Kommission außerdem Vorschläge für Rechtsakte zur Erweiterung des *Schengener Informationssystems* (SIS) von einer polizeilichen Ausschreibungsdatei zur einem umfassenden Europäischen Polizeilichen Informationssystem (SIS II) vorgelegt. Diese Vorschläge würden bei einer unveränderten Annahme die Wahrnehmung von grundlegenden Datenschutzrechten der Unionsbürgerrinnen und -bürgern auf Auskunft, Berichtigung und Löschung ebenso erschweren wie eine effektive Datenschutzkontrolle. Es ist von entscheidender Bedeutung, dass diese Rechtsakte unter Berücksichtigung der Vorschläge verabschiedet werden, die die Europäischen Datenschutzbeauftragten im Rahmen der Art. 29-Gruppe[11] formuliert haben, und nur zeitgleich mit dem erwähnten Rahmenbeschluss über den Datenschutz in der dritten Säule. Die Intensivierung der polizeilichen Zusammenarbeit in Europa muss Hand in Hand gehen mit einer Harmonisierung der Datenschutzbestimmungen und einer effektiveren Datenschutzkontrolle.

9 BR-Drs. 764/05
10 BR-Drs. 770/05
11 WP 116, abrufbar unter http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp116_en.pdf

1.2 Deutschland

Das *Bundesverfassungsgericht* hat sich im Berichtszeitraum in zwei Entscheidungen mit Grundfragen des Datenschutzes befasst. Zum einen hat es die Grenze des Einsatzes verdeckter technischer Ermittlungsmethoden im Strafverfahren präzisiert und zum anderen hat es sich zu den Grenzen der präventiven Telekommunikationsüberwachung geäußert.

In seinem Urteil zum Einsatz des *Global Positioning Systems* (GPS)[12] hat das Gericht den Einsatz dieser modernen Methode zur *Observation* von Verdächtigen zwar prinzipiell gebilligt, zugleich aber Grundsätze für den gleichzeitigen Einsatz mehrerer Ermittlungsmaßnahmen formuliert, die Bedeutung über diesen Fall hinaus haben. Zum einen müssen die Strafverfolgungsbehörden zum gleichzeitigen Einsatz mehrerer Überwachungsmethoden gegen einen Verdächtigen besondere verfahrensmäßige Anforderungen beachten, um das Gefährdungspotenzial zu begrenzen, das einem solchen „additiven“ Grundrechtseingriff innewohnt. Zum anderen muss der Gesetzgeber wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam beobachten und notfalls durch ergänzende Rechtssetzung korrigierend eingreifen. Das betrifft insbesondere auch die Frage, ob die bestehenden rechtlichen Vorkehrungen angesichts des technologischen Wandels den Grundrechtsschutz hinreichend effektiv sichern können. In der mündlichen Verhandlung, die diesem Urteil vorausging, wurde der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Dr. Garstka, als Sachverständiger gehört.

Der Hinweis des Bundesverfassungsgerichts auf die Risiken „additiver“ Grundrechtseingriffe ist auch für die Gesetzgebung bedeutsam: Viele der in den letzten Jahren kontinuierlich beschlossenen Befugniserweiterungen für die Sicherheitsbehörden mögen für sich genommen legitim erscheinen. Betrachtet man das Gesamtbild, ist jedoch eine deutliche Tendenz in Richtung einer *Rundumüberwachung* der Menschen festzustellen, die nach der wiederholten Aussage des Bundesverfassungsgerichts mit dem Grundgesetz unvereinbar ist[13].

In seiner grundlegenden Entscheidung zum Niedersächsischen Polizeigesetz[14] hat das Bundesverfassungsgericht klargestellt, dass die Länder keine Gesetzgebungskompetenz für Maßnahmen zur Vorsorge für die Verfolgung künftiger Straftaten haben. Diese Aussage hat weitreichende Auswirkungen für die Polizeigesetzgebung auch in Berlin. Denn das Allgemeine Sicherheits- und Ordnungsgesetz (§ 1 Abs. 3) weist der Polizei auch die Aufgabe zu, für die Verfolgung künftiger Straftaten vorzusorgen. Auch materiell hat das Bundesverfassungsgericht die Befugnis zur *präventiven Telekommunikationsüberwachung* im Niedersächsischen

12 v. 12. April 2005, BVerfGE 112, 304
13 BVerfG 112, 304, 319
14 Urteil v. 27. Juli 2005 – 1 BvR 668/04, NJW 2005, 2603

Landesrecht für verfassungswidrig erklärt. Es hat seine Forderung bekräftigt, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben müssen[15]. Auch insoweit muss das Berliner Polizeigesetz der Verfassungsrechtsprechung noch angepasst werden, auch wenn es die präventive Telekommunikationsüberwachung bisher nicht zulässt. Sowohl die *akustische Wohnraumüberwachung* als auch der Einsatz verdeckter Ermittler müssen den absolut beschützten Kernbereich privater Lebensgestaltung respektieren. Gleiches gilt für das Berliner Verfassungsschutzgesetz, das solche expliziten Sicherungen bisher ebenfalls nicht enthält.

In einer bemerkenswerten Entscheidung hat der *Bundesgerichtshof* die Verwertung eines in einem Krankenzimmer geführten *Selbstgesprächs*, das mittels akustischer Wohnraumüberwachung aufgezeichnet wurde, in einem Strafverfahren wegen Mordes untersagt[16]. Zum einen gehöre auch ein Krankenzimmer zur verfassungsrechtlich nach Art. 13 GG geschützten „Wohnung“. Zum anderen habe ein Selbstgespräch ausschließlich höchstpersönlichen Charakter und sei dem Kern privater Lebensgestaltung zuzurechnen, in den nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich nicht eingegriffen werden dürfe. Das gilt nach Auffassung des Bundesgerichtshofs umso mehr, als der Betroffene seine heimlich belauschte Äußerung nicht einem anderen („Zwiegespräch“) gegenüber gemacht hat, sondern lediglich laut gedacht hat. Zudem habe er seine Gedanken auch nicht einem Tagebuch anvertraut und damit der Gefahr eines Zugriffs ausgesetzt. Bei der Verwertung von Tagebuchaufzeichnungen im Strafprozess hat das *Bundesverfassungsgericht* einen Verstoß gegen das Grundgesetz dagegen verneint[17].

Der Bundesgesetzgeber hat im Berichtszeitraum zum einen die Strafprozessordnung an Vorgaben des Bundesverfassungsgerichts in der Lauschangriffsentscheidung vom März 2004 angepasst, wobei er allerdings zunächst nur die Regelungen über die akustische Wohnraumüberwachung modifiziert hat[18]. Die notwendige entsprechende Begrenzung der Befugnis zur Überwachung von Telekommunikation steht noch aus. Zum anderen ist der Einsatzbereich des sog. genetischen Fingerabdrucks im Strafprozess erneut erheblich ausgeweitet worden[19].

Als erster Mitgliedstaat der Europäischen Union führte die Bundesrepublik zum 1. November 2005 den *biometrischen Reisepass* ein, der zunächst auf einem integrierten RFID-Chip das digitalisierte Passfoto, voraussichtlich ab 2007 auch Fingerabdrücke des Passinhabers enthält. Damit setzte sich die Bundesregierung über die Bedenken der Datenschutzbeauftragten

15 so schon die Entscheidung zum Großen Lauschangriff v. 3. März 2004, BVerfG 109, 279 vgl. dazu JB 2004, S. 11
16 Urteil v. 10. August 2005 – 1 StR 140/05, NJW 2005, 3295
17 BVerfGE 80, 367
18 vgl. 4.3.1
19 vgl. 4.3.1

hinweg, die auf weiterhin bestehende Sicherheitsrisiken mit dieser weltweit bisher noch nicht eingesetzten Technologie hinwiesen[20]. Noch ist völlig ungeklärt, wie sichergestellt werden kann, dass Passdaten bei der Einreise in andere Länder ohne hinreichendes Datenschutzniveau vor einer Zweckentfremdung geschützt werden können. Ohnehin wird nicht mehr ernsthaft behauptet, dass die Einführung biometrischer Reisepässe ein wirksamer Beitrag im Kampf gegen den internationalen *Terrorismus* sei, denn die meisten Attentäter des 11. September 2001 verfügten bekanntlich über echte Reisepässe.

1.3 Berlin

In Berlin hat der Gesetzgeber im Berichtszeitraum eine Reihe von gesetzlichen Regelungen beschlossen, die Auswirkungen auf den Datenschutz und die Informationsfreiheit haben.

So wurde durch das Vierte Gesetz zur Reform der Berliner Verwaltung vom 3. November 2005 eine Vorschrift in das Bezirksverwaltungsgesetz eingefügt, die die *informationelle Gewaltenteilung* innerhalb der *Bürgerämter* entsprechend dem funktionalen Behördenbegriff festlegt. Durch das Gesetz zur Vereinfachung des Berliner Baurechts vom 29. September 2005 wurden in die *Bauordnung für Berlin* Vorschriften zur Datenverarbeitung eingefügt, die weitgehend auf unseren Vorschlägen beruhten. Durch das *Gesetz zur Errichtung einer Ethik-Kommission des Landes Berlin* von 7. September 2005 wurde in Berlin in einem der ersten Bundesländer ein Gremium zur ethischen Beurteilung von Forschungsvorhaben eingerichtet, mit dessen Tätigkeit sich für uns künftig vielfache Berührungspunkte ergeben werden[21]. Für den Bereich der Grundsicherung und der Asylbewerberleistungen sieht das *Gesetz zur Ausführung des Zweiten Buches Sozialgesetzbuch und Zwölften Buches Sozialgesetzbuch vom 7. September 2005* Möglichkeiten des Datenabgleichs und des automatisierten Abrufverfahrens vor[22]. Das *Erste Gesetz zur Änderung des Gesetzes über das Halten und Führen von Hunden in Berlin vom 23. Juni 2005* regelt die im vergangenen Jahr angesprochenen[23] offenen Fragen der Verwendung der Daten von Hundehaltern für die private Rechtsverfolgung oder für die Ordnungs-, Polizei- und Steuerbehörden.

Außerdem wurde kurz vor dem Ende des Berichtszeitraums das *Informationsfreiheitsgesetz* durch einen Verweis auf das neue Umweltinformationsgesetz des Bundes ergänzt, so dass Umweltinformationen in Berlin zukünftig in der gleichen Weise offen gelegt werden müssen, wie es für die Bundesrepublik insgesamt durch Europäisches Gemeinschaftsrecht vorgeschrieben

20 vgl. 2.1
21 GVBl., 466; vgl. 6.2
22 GVBl., 467
23 JB 2004, 1.2

ist[24]. Schließlich legte das Abgeordnetenhaus im *Vergütungs- und Transparenzgesetz* vom 23. September 2005[25] Kriterien für eine größere Transparenz bei den *Vorstandsvergütungen* der Berliner Anstalten und den Geschäftsführungsvergütungen bei Beteiligungen Berlins an privatrechtlichen Unternehmen fest. Entsprechende Regelungen hat die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland auch für alle anderen Bundesländer gefordert[26]. Damit würde auch ein Anliegen unterstützt, dass der Bundesgesetzgeber mit der Verabschiedung des Gesetzes über die Offenlegung von Vorstandsvergütungen bei Kapitalgesellschaften verfolgt[27]. Das *16. Gesetz zur Änderung des Landesabgeordnetengesetzes vom 3. November 2005*[28] enthält detaillierte Regelungen für die Offenlegung von Nebentätigkeiten von Abgeordneten sowie über die Rechnungslegung und Anzeigepflicht bei Spenden.

24 GVBl. 2005, 791; vgl. 6.
25 GVBl., 475
26 vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, B I. 2
27 vgl. 6.1
28 GVBl., 690

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Entwicklungstendenzen

Betrachtet man die Werbung der Elektronik-Discounter für neue Computer für das traute Heim, so fallen zwei Dinge auf: Zum einen hat sich das Tempo der Weiterentwicklung von schnellen Prozessoren offensichtlich verlangsamt, zum anderen steigt der Bedarf und auch das Angebot an Speicherplatz erheblich an. Leistungsstarke Prozessoren haben heute eine Taktfrequenz von ca. 3,5 GHz, nur wenig mehr als im Vorjahr. Die Kapazitäten der Arbeitsspeicher und Festplatten der angebotenen Rechner steigen jedoch immens an. Ausstattungen von 2 GB Arbeitsspeicher und 200 GB Festplatte repräsentieren den gehobenen Standard.

Wie schon in den Vorjahren an dieser Stelle festgestellt wurde, hat sich die Nutzung der privaten Heimcomputer grundlegend gewandelt. Die Rechner sind Teil der Aufrüstung der privaten Mediennutzung. Riesige Speicherkapazitäten sind notwendig, um Spielfilme und Musikstücke digital zu speichern, um Videos und Digitalfotografien zu sammeln und zu bearbeiten. Zubehörteile für die Befriedigung des privaten Unterhaltungsbedürfnisses haben die PCs längst von der Spitze der Weihnachtswunschlisten verdrängt. MP3-Player, Speichersticks, Spielkonsolen, Digitalkameras, Fotodrucker, ganz zu schweigen von DVD-Abspielgeräten und -Rekordern waren die Renner des Weihnachtsgeschäfts 2005.

Auffällig ist, dass sich diese Entwicklung von den Tendenzen im Bereich der professionellen Datenverarbeitung deutlich abkoppelt. Im beruflichen Zusammenhang spielen speicherfressende Anwendungen keine große Rolle. Auch moderne Bürosysteme, mit denen die Vision des papierlosen Büros umgesetzt werden soll, haben trotz der massenhaften Ablage gescannter Dokumente kaum eine dem Home Entertainment vergleichbare Speicherdichte. Auch die berufliche Nutzung des Internet erhöht den Ressourcenbedarf nicht erheblich.

Anders als zu Hause, wo die elektronische Unterhaltung eher vereinsamende Effekte beschleunigt, spielt im Arbeitsleben die Vernetzung von Systemen eine große Rolle. Zusammenarbeit und elektronische Kommunikation, der dezentrale Zugriff auf zentrale Ressourcen, beeinflussen hier die Entwicklungstendenzen. Nicht die konzentriert im Wohnzimmer stehende Masse spielt eine Rolle, sondern die Erreichbarkeit von Informationen, wo und wann sie gebraucht werden. In den Büros kommt es darauf an, aus dem Überangebot von Daten diejenigen zu finden, die man gerade braucht. Hierin besteht die Herausforderung für

die Zukunft, die auch weiter die Entwicklungstendenzen in der professionellen Datenverarbeitung bestimmen wird.

Ein Beispiel mag das deutlich machen. Ein aktueller Discounter-Computer von gehobener Ausstattung hat genügend Speicherkapazität, um die Daten des Berliner *Einwohnerregisters* aufzunehmen, dennoch kann es nur funktionieren, wenn Hunderte vernetzte Computer dabei eingesetzt werden. Diese Computer brauchen nicht annähernd die quantitative Ausstattung der häuslichen Zentrale der Unterhaltungselektronik.

Diese Überlegungen haben dazu geführt, dass sich die Ausstattung der Arbeitsplatzcomputer in die gegengesetzte Richtung entwickelt hat, vergleicht man es mit der Ausstattung der Homecomputer. Die Entwicklung immer leistungsstärkerer Systeme führt dazu, die Leistungen der Bürosysteme auf schnelle zentrale Server mit großen Speicherkapazitäten zu konzentrieren und sie mittels abgespeckter dezentraler Systeme dort anzubieten, wo sie gebraucht werden. Die Lastverteilung zwischen Clients und Servern verlagert sich verstärkt zu den Servern. Während die Leistungsanforderungen an zentrale Systeme vom quantitativen Trend im privaten Sektor profitieren und im qualitativen Bereich – vor allem bei der Sicherstellung der Verfügbarkeit – höhere Maßstäbe setzen, benötigt man dezentral nur noch abgespeckte Systeme, die den Zugang zu den Servern in effizienter und ergonomischer Weise ermöglichen. Die je nach Hersteller anders betitelten „*Terminal Server“-Systeme*, „*Server Based Computing*“-*Systeme* oder „*Thin Clients*“ sind auf dem Vormarsch und lösen die immer noch gängigen Client-Server-Netze ab.

Diese Entwicklung berührt auch die IT-Sicherheit und damit den Datenschutz. Durch die Rückkehr der zentralen Datenverarbeitung steigen die Sicherheitsanforderungen in der Zentrale. Auf Ausweichlösungen mit den dezentralen Rechnern kann man bei Terminal-Server-Lösungen nicht mehr hoffen, wenn das zentrale System ausfällt. Die Anforderungen an die Verfügbarkeit der zentralen Systeme steigen, während sie für die dezentralen Systeme sinken. Risiken für die Vertraulichkeit und Integrität der Daten konzentrieren sich in der Zentrale, die damit stärker in den Fokus der IT-Sicherheitserwägungen gezogen wird.

Andererseits reduzieren sich die Risiken, die sich aus den Missbrauchspotenzialen leistungsstarker Arbeitsplatzsysteme ergeben, weil der Eingriff in Verarbeitungsprozesse durch die Verlagerung dieser Prozesse auf zentrale Systeme entscheidend erschwert, wenn nicht unmöglich gemacht wird.

„IT-Lokomotive“ Staat

Seit Jahren wird der Durchbruch biometrischer Authentifizierungssysteme in der praktischen Anwendung erhofft. Im Zusammenhang mit dem Homebanking und dem Umgang mit Geld-automaten wird sehnsüchtig auf die Ablösung der bekannt unsicheren Verfahren mit PIN und TAN durch sichere biometrische Verfahren gewartet. Auch die hektischen Vermarktungs-aktivitäten einschlägiger Anbieter biometrischer Systeme nach den Anschlägen vom 11. September 2001 haben es nicht vermocht, die Technologie zu praktischer Verbreitung zu bringen.

Dies kann sich jetzt ändern: Nach der Zweiten Verordnung zur Änderung passrechtlicher Vorschriften[29] wurde durch die Bundesregierung bestimmt, dass *Reisepässe*, die nach dem 1. November 2005 beantragt werden, über einen Speicherchip verfügen, der das digitalisierte Lichtbild enthält. Ab 2007 soll der *digitalisierte Fingerabdruck* hinzukommen. Bei Grenz-kontrollen soll dann das gespeicherte Abbild und später der gespeicherte Fingerabdruck mit der realen Person verglichen werden und so automatisiert festgestellt werden, ob es sich um die gleiche Person handelt. Diese Entscheidung des Verordnungsgebers ersetzt alle bisherigen Hemmnisse bei der Verbreitung biometrischer Erkennungsverfahren, die darin bestehen, dass sie die notwendige Verlässlichkeit bei der Authentifizierung noch nicht erbringen. Neben den vielen datenschutzrechtlichen Bedenken, die gegen die Einführung des ePasses vorgebracht wurden, bleibt ein grundsätzliches Problem immer bestehen: *Biometrische Erkennungs-verfahren* sollen zwei Muster als gleich oder ungleich erkennen, die stets nicht gleich, sondern nur ähnlich sein können. Es kommt also darauf an, mit automatischen Verfahren festzustellen, ob eine Ähnlichkeit als Gleichheit, Ungleichheit oder Klärungsfall zu werten ist. Solche Systeme können justiert werden, bei welchem Ähnlichkeitsgrad die Erkennung verneint oder bejaht wird. Aus Sicherheitsgründen scharf eingestellte Systeme verweigern also die Erkennung im Zweifel, so dass beim Grenzübertritt zwar eine Täuschung des Verfahrens unwahrscheinlich ist, dafür aber viele Personen unberechtigterweise (zunächst) zurückgewiesen werden. Will man das durch Verringerung der Schärfe vermeiden, besteht die Gefahr, dass unberechtigte Grenz-übertritte erfolgen.

Die Entscheidung der Bundesregierung, jetzt biometrische Reisepässe auszugeben, enthält also einen Wechsel auf die zukünftige Entwicklung der biometrischen Erkennungssysteme, wird aber auch gleichzeitig einen zusätzlichen Motivationsschub für die Entwickler mit sich bringen. Ob dadurch tatsächlich die innere Sicherheit erhöht wird, bleibt abzuwarten. Indirekt könnte diese Entscheidung immerhin dazu beitragen, dass auch im Wirtschaftsleben eine zuverlässigere Personenauthentisierung möglich wird.

29 BGBl I 2005, 2306 ff.

Auch auf einem anderen Technologiefeld sorgt Vater Staat für die lang ersehnten und in vielen Kongressen beschworenen „Killer Applications“, die endlich die Fesseln beseitigen sollen, die bisher der Marktdurchdringung entgegenstanden. *Intelligente Chipkarten* (Prozessorchipkarten) sind im Gegensatz zu den einfachen Speicherchipkarten (Telefonkarten, Geldkarten, Krankenversicherungskarten) noch nicht in jeder Brieftasche (aber im Handy). Dies liegt nicht am Stand der Technologie, die als ausgereift gelten kann, sondern am Mangel an Anwendungsmöglichkeiten, die es den Kunden leicht machen würden, nach solcher Technik zu verlangen.

Zu nennen sind an dieser Stelle neben den chipbestückten biometrischen Reisepässen die *JobCard* und die *elektronische Gesundheitskarte*.

Nach dem Beschluss der Bundesregierung vom 21. August 2002 soll für alle Arbeitnehmer eine JobCard eingeführt werden, mit deren Hilfe die Arbeitsverwaltung auf Beschäftigungszeiten, Entgelte und Angaben zur Auflösung des Beschäftigungsverhältnisses, also auf die Arbeitsbescheinigungen nach § 312 SGB III, elektronisch zugreifen kann. Die Bezeichnung „JobCard-Verfahren“ täuscht darüber hinweg, dass es sich eigentlich nicht in erster Linie um ein Chipkartenprojekt handelt, sondern um den Aufbau einer Zentralen Speicherstelle, die alle elektronischen Arbeitsbescheinigungen aller Arbeitnehmer an zentraler Stelle zusammenführt. Für den Fall, dass der Arbeitnehmer Sozialleistungen beantragen will, autorisiert er bei der Beantragung der Sozialleistungen den Sachbearbeiter zum Abruf der relevanten Daten bei der Zentralen Speicherstelle, indem er seine gültige Signaturkarte aktiviert und sich so dem System gegenüber authentifiziert. Gleiches muss der Sachbearbeiter tun, um sich als empfangsberechtigt zu identifizieren.

Es geht an dieser Stelle nicht um die datenschutzrechtliche Bewertung des Verfahrens, sondern um die Feststellung, dass der zitierte Beschluss der Bundesregierung dazu führen würde, dass sich jeder Arbeitnehmer eine solche Signaturkarte für die qualifizierte digitale Signatur beschaffen muss. Dabei kommt es nicht darauf an, von welchem Trust Center die Karte ausgegeben wird. Jede beliebige Signaturkarte für die qualifizierte Signatur dient als JobCard. Bedenkt man, dass solche Signaturkarten bisher höchst sporadisch verkauft wurden, weil es noch nicht genügend Anwendungen dafür gibt, dürfte die Einführung des JobCard-Verfahrens hier den Durchbruch erbringen, also auch hier erfolgt die Marktdurchdringung durch eine Entscheidung „von oben“.

In den gleichen Zusammenhang kann das Vorhaben zur Einführung einer *elektronischen Gesundheitskarte* (eGK) eingeordnet werden.

Mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung wurde u. a. das Sozialgesetzbuch V um § 291 a ergänzt. Diese Vorschrift sieht vor, dass spätestens zum

1. Januar 2006 die bisherige *Krankenversichertenkarte* zu einer elektronischen Gesundheitskarte erweitert wird. Der in der Vorschrift detailliert dargestellte Funktionsumfang umfasst neben der Aufnahme der Daten der bisherigen Versichertenkarte die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form sowie den Berechtigungsnachweis zur Inanspruchnahme von Leistungen und der Speicherung von Notfalldaten auch die Öffnung des Netzzugangs an persönliche Daten, die nicht auf der Karte, sondern in anderen Systemen gespeichert werden, zum Beispiel elektronische Arztbriefe und Patientenakten. Dieser Funktionsumfang und die Techniken zur Absicherung der technisch-organisatorischen Datenschutzziele lassen sich nur mit prozessorgesteuerten Chipkarten realisieren.

Auch an dieser Stelle soll es nicht um eine datenschutzrechtliche Bewertung dieses hochkomplexen Verfahrens gehen, sondern es soll die trendsetzende Rolle der Bundesregierung herausgehoben werden, die die Entwicklung der *Prozessor-Chipkarten* durch gesetzlichen Zwang forciert. Es gibt Hinweise, dass es sich bei der elektronischen Gesundheitskarte um das größte und komplexeste IT-Projekt in der Geschichte der Bundesrepublik handelt, weit größer als das Projekt zur Einführung der Autobahnmaut. Daher war bereits früh abzusehen, dass der in § 291 a Abs. 1 Satz 1 SGB V gesetzte Termin nicht zu halten war.

Aktuelle Entwicklung und Einsatz der RFID-Technologie

Die Einführung der *RFID-Technologie* im Einzelhandel als Ergänzung und bald auch als Nachfolger der Barcode-/Strichcode-Technologie steht kurz bevor. Nachdem dieses Thema im Jahresbericht 2004 einen Schwerpunkt darstellte und ausführlich beschrieben wurde[30], soll hier über die weitere Entwicklung dieser zukunftsträchtigen und datenschutzrechtlich relevanten Technologie berichtet werden. Zum Einsatz dieser Technik bei der Fußballweltmeisterschaft 2006 in Deutschland kommen wir in Abschnitt 4.1 zurück.

RFID – die Abkürzung für Radio Frequency Identification – wird als Oberbegriff für die komplette technische Infrastruktur verwendet. Ein RFID-System umfasst in der Regel:

- den Transponder (auch RFID-Etikett, -Chip, -Tag, -Label, Funketikett oder -chip genannt),
- die Sende-Empfangs-Einheit (auch Reader genannt),
- die Integration mit Servern und sonstigen Systemen wie z. B. Kassensysteme oder Warenwirtschaftssysteme (also die Weiterverarbeitung der Daten mit einer Datenbank im Hintergrund).

30 JB 2004, 3.4

Da die Kompatibilität der einzelnen Komponenten für eine flächendeckende weltweite Markteinführung eine entscheidende Rolle spielt, hat die International Organization for Standardization (ISO) die Aufgabe der internationalen Normung übernommen. ISO-Standards legen beispielsweise Frequenzen, Übertragungsgeschwindigkeiten und Kodierungen für RFID-Systeme fest. So handelt es sich bei dem bei der Fußball-WM verwendeten ISO-Standard 14443 um einen ultraflachen Chip (auch *Smart Card* genannt), der samt Antenne auf die Tickets aufgebracht werden kann.

Bisher war dem Verbraucher diese in der Logistik schon seit längerer Zeit eingesetzte RFID-Technik weitgehend unbekannt, bei der alle mit einem *RFID-Etikett* (im Folgenden: *RFID-Tag*) versehenen Waren über Funkwellen erkannt und identifiziert werden können. Da ein einzelner passiver RFID-Tag über einen 96-Bit-Speicher verfügt, kann jedes mit einem solchen Tag ausgestattetes Produkt weltweit individuell gekennzeichnet werden. Die RFID-Technik wird allerdings schon seit Jahren in der Wirtschaft, speziell in der Logistik bei der Warenverfolgung oder zur Gewährleistung der Kühlkette, eingesetzt. Ebenso findet sie seit langer Zeit schon als *Wegfahrsperre* bei PKWs, in *Skipässen*, bei der Tieridentifikation und zur Kennzeichnung von Büchern in Bibliotheken Verwendung. In der öffentlichen Diskussion werden allerdings Szenarien zur Leistungsfähigkeit der RFID-Technologie beschrieben, die gegenwärtig noch nicht realistisch sind. Es ist noch eine ganze Reihe technischer Hürden zu überwinden, bevor z. B. Waren mit RFID-Tags in einer Einkaufstüte identifiziert und kontaktlos beim Passieren der Kasse der Gesamtpreis berechnet werden kann. Die Gefahr, dass die Einkaufstüte mit bezahlten Waren nach dem Verlassen des Supermarkts von Dritten durchleuchtet und damit personenbezogene Konsumprofile erhoben werden, wird erst dann konkret, wenn Lesegeräte zum unbemerkten Auslesen der Funkchips eingesetzt werden können.

Wie bei jeder neuen Technikeinführung in den breiten Markt muss man jedoch auch bei der RFID-Technologie differenzieren. Eine Bewertung aus technischer und datenschutzrechtlicher Sicht ist daher nicht allgemein, sondern nur auf den konkreten Anwendungsfall möglich. RFID-Tags unterscheiden sich teilweise recht stark voneinander. Sie können durchaus die Größe von Büchern haben (z. B. in der Containerlogistik), aber auch sehr klein und dünn sein, so dass sie in Geldscheinen oder Papier eingebettet werden können. Ihre Leistungsfähigkeit ist immer abhängig von ihrer Verwendung bzw. ihrem Anwendungsgebiet. Der Aufbau eines RFID-Tags sieht prinzipiell eine Antenne, einen analogen Schaltkreis zum Empfangen und Senden (Transponder) sowie einen digitalen Schaltkreis und einen permanenten Speicher vor. Abhängig vom jeweiligen Anwendungsbereich kann es aber erhebliche Unterschiede hinsichtlich Funkfrequenz, Übertragungsrate, Lebensdauer, Kosten pro Einheit, Speicherplatz, Lesereichweite und Funktionsumfang geben.

Erst die kritische öffentliche Diskussion über die Risiken der RFID-Tags hat im letzten Jahr dazu geführt, dass die Hersteller verstärkt über eine datenschutzgerechte Gestaltung und Einsatzweise dieser Technologie nachdenken. So werden jetzt einfache Möglichkeiten der Abschaltung (Deaktivierung) von Funkchips nach dem Kauf der entsprechend markierten Waren z. B. durch das Abreißen der Antenne erwogen. Solche „Low Tech“-Lösungen haben durchaus Vorzüge im Hinblick auf *Transparenz* und Nutzerfreundlichkeit. Prinzipiell sollte aber derjenige für eine nachvollziehbare Deaktivierung des RFID-Etiketts sorgen, der es an der Ware angebracht hat, also z. B. der Verkäufer. Die Verantwortung dafür sollte grundsätzlich nicht auf den Käufer abgewälzt werden. Ausnahmen sind allenfalls bei hochwertigen Gegenständen denkbar, bei denen der Käufer den Chip nach dem Kauf zunächst deaktivieren, später aber zur Geltendmachung von Gewährleistungsansprüchen ohne Kaufbeleg wieder aktivieren will (z. B. bei einer Armbanduhr).

Tatsache ist, dass die RFID-Technologie in den nächsten Jahren den Barcode vollständig ersetzen wird und durch seine technischen Ausprägungen, Anpassungs- und Einsatzmöglichkeiten vor allem den Einzelhandel revolutionieren könnte. In diesem Zusammenhang wird auch bargeldloses Bezahlen weiter vorangetrieben, was nicht nur zu einer Veränderung der Beschäftigungsstruktur im Einzelhandel (aufgrund der Einsparung beim Kassenpersonal), sondern auch zu erhöhten datenschutzrechtlichen Risiken führen wird. Diese müssen durch eine entsprechende Gestaltung der Technik bereits in der Entwicklungsphase beherrscht werden.

RFID bei der Fußball-WM 2006

Die *RFID-Technologie* soll ihren ersten großen bundesweiten Auftritt bei der *Fußball-Weltmeisterschaft* 2006 haben, bei der in jedes Ticket ein individueller RFID-Tag integriert wird und damit jeder Stadionbesucher identifiziert werden könnte. In diesem Zusammenhang sandte uns das Organisationskomitee (OK) des Deutschen Fußballbundes auf unsere Nachfrage seine Konzeption *„Ticketpersonalisierung und Sicherheitsüberprüfungen am Stadion für FWC“* (Football World Cup) vor. Daraus ergibt sich Folgendes:

Der konkrete Einsatz der RFID-Technologie bei der Fußball-WM 2006 in Deutschland und damit die Möglichkeit des Zugangs zu den Stadien ausschließlich mit personalisierten Tickets ist grundlegender Bestandteil des von der „Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK)“ verabschiedeten Sicherheitskonzepts. Konkret bedeutet dies, dass von jedem Ticket-Besteller und Besucher (mindestens) folgende personenbezogene Daten erhoben werden: Name, Vorname, Nationalität, Geburtsdatum und Reisepass-Nummer. Diese Mindestangaben gelten für alle für den Verkauf auszugebenden Tickets. Diese und sämtliche über die Ticketbestellformulare erhobenen Daten werden in der *Ticketdatenbank* gespeichert. Zum Teil werden diese Daten schon während der Erhebung mit den in der Stadionverbotsdatei das DFB gespeicherten Daten verglichen, zum Teil erst zu einem späteren Zeitpunkt wie z. B. vor dem Druck der Tickets oder bei der Übertragung der Daten in die Datenverarbeitungsanlage des Stadions im Vorfeld der eigentlichen Veranstaltung.

Im Regelfall werden von den erhobenen personenbezogenen Daten nur die Gruppenzuge-hörigkeit, der Vor- und Nachname des Kunden und die Nationalität auf das Ticket gedruckt; alle weiteren erhobenen Daten werden in der Ticketdatenbank gespeichert. Sollte zum Zeitpunkt des Ticketdrucks der Name des Kunden noch nicht feststehen (z. B. wenn Tickets zu Gewinn-spielen eingesetzt werden und der Gewinner erst später ermittelt werden kann), so wird anstelle des Namens eine Kunden-Nummer als Referenz auf das Ticket gedruckt. Auf Basis dieser Kunden-Nummer muss eine Nachpersonalisierung im Regelfall bis spätestens eine Woche vor dem betreffenden Spiel erfolgt sein. Diese Regelung gilt auch für die so genannten Sponsorentickets, die nicht in den freien Verkauf gelangen, sondern den Sponsoren zur weiteren Verwendung zur Verfügung gestellt werden. Kunden mit nichtpersonalisierten Tickets wird bei der Kontrolle durch das elektronische Zugangskontrollsystem im Eingangsbereich der Stadien der Einlass verweigert.

Alle Tickets sind mit einem RFID-Tag gemäß ISO 14443 ausgestattet. Da der in jedem Ticket integrierte Tag über eine eindeutige ID-Nummer verfügt, ist eine Fälschung nicht möglich. Die in der Ticketdatenbank gespeicherten Daten sind über die vorhandene eindeutige Tag-ID einer Eintrittskarte zugeordnet. Direkt personenbezogene Daten werden im Tag selbst nicht

gespeichert, die Daten sind jedoch durch die eben genannte Zuordnung über die Ticketdatenbank auf die Person beziehbar.

Das gesamte Verfahren der Ticketpersonalisierung führen das OK des DFB und seine Auftragnehmer (private Event-Organisatoren) als verantwortliche Stellen durch.

Der erstmalige flächendeckende Einsatz der RFID-Technologie bei der Fußball-WM 2006 wirft aber auch die grundsätzliche Frage auf, ob in Zukunft bei allen Großveranstaltungen ein der-artiger Zwang zur Identifizierung gelten soll. Die Datenschutzbeauftragten des Bundes und der Länder haben sich dagegen ausgesprochen und betont, dass die personalisierte Ticketvergabe bei Fußball-WM nicht zum Vorbild für sportliche und andere Großveranstaltungen werden darf[31].

Erstaunliches und Skurriles

Verfolgt man die einschlägigen papierenen und elektronischen Magazine, so liest man über viele Ideen und Entwicklungen, die zunächst erstaunen, vielleicht sogar belustigen. Dies soll an dieser Stelle nicht geschehen, denn so manche erstaunliche und skurril erscheinende Idee in der Informationstechnik hat später den Siegeszug durch die Welt angetreten. Über solche Ideen soll hier kurz berichtet werden.

Eine Berliner Tageszeitung berichtete über einen Professor aus Tokio, dem es gelungen war, mit einem speziellen Laser unsichtbare Muster in Fingernägel hineinzuschmelzen und so Daten bis zu 5 MB auf den Fingernagel aufzutragen. Die Fingernägel werden zum Lesen der Daten mit ultraviolettem Licht angestrahlt und die Daten können dann mit einer Kamera und einem Fluoreszenzmikroskop gelesen werden. Der Datenschutz spielte bei diesem Projekt eine überraschend vielseitige Rolle: Motiviert wurde der Professor, weil er sich nicht alle seine PIN-Codes und Passwörter merken wollte und nach einer Methode suchte, um die Daten immer bei sich zu haben. Da die Fingernägel nachwachsen, ist die Speicherdauer automatisch begrenzt, nach sechs Monaten ist alles herausgewachsen. Auf diese Weise wird der Professor daran erinnert, bei der Neuspeicherung gleich die regelmäßige Änderung der Zugangsdaten vorzunehmen. Der Artikel weist ausdrücklich darauf hin, dass die abgeschnittenen Fingernägel

31 Entschließung der 69. Konferenz v. 11./12. März 2005: „Datenschutzbeauftragte plädieren für die Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 10

einer Vernichtung zugeführt werden müssen, um dem Datenmissbrauch vorzubeugen.

Ein überregionales Blatt berichtet von Forschern der Technischen Universität Berlin, die sich mit *organischen Computern* befassen, die biologische Prozesse nachahmen, um sich selbst zu organisieren, zu optimieren, zu reparieren und an die Umgebung anzupassen. Experten gehen davon aus, dass organisches Computing in fünf Jahren anwendungsreif sein kann, z. B. im Rahmen einer „*Smart Factory*“, in der sich Computer nach Bedarf vernetzen, Störungen beseitigen und Aufgaben spontan verteilen.

In den USA erwägen Pharma-Unternehmen nicht nur jede Packung der von ihnen produzierten Arzneimittel, sondern auch jede einzelne Pille mit einem *RFID-Etikett* zu versehen, um sich vor Schadensersatzforderungen bei der Einnahme von Nachahmerprodukten zu schützen. In diesem Zusammenhang ist auch der künftige Einsatz von RFID-Tags in Kombination mit Sensortechnologie zu sehen, die in den Körper eines Patienten implantiert oder eingeführt werden, um seinen Gesundheitszustand zu kontrollieren und ihm bei Bedarf die erforderlichen Dosen eines Arzneimittels zuzuführen (z. B. die Insulin-Dosierung bei Zuckerkranken).

Völlig ohne Funkübertragung kommt die *Sensortechnologie* Skinplex aus, bei der die menschliche Haut als Medium der Datenübertragung dient. Ein Signalgeber in der Hosentasche eines Autofahrers ändert die Oberflächenspannung seiner Haut geringfügig, was von speziellen Sensoren im Türgriff des Autos empfangen und erkannt wird.

Damit würden herkömmliche Funkschlüssel überflüssig, die insofern ein Sicherheitsrisiko bergen, als ihre Signale mit einfachen Mitteln (z. B. einer Richtfunkantenne in zwanzig Meter Entfernung) abgehört werden können.

Insbesondere die Entwicklung der Sensortechnik wird den Datenschutz in naher Zukunft vor völlig neue Herausforderungen stellen.

2.2 Datenverarbeitung in der Berliner Verwaltung

Wie schon in den Vorjahren ist der durch die finanzielle Situation des Landes erzwungene Stellenabbau in der Berliner Verwaltung verbunden mit einer stetigen Erweiterung und Modernisierung der informationstechnischen Ausstattung und der Erschließung neuer Anwendungen zur Verbesserung der Bürgerfreundlichkeit und der Arbeitssituation an den verbliebenen Arbeitsplätzen. Die im Vorjahr initiierte Reform der IT-politischen Strukturen ist im Lande vorangetrieben worden. Die Effekte dieser Reform auf die sehr anspruchsvollen Ziele der

Berliner IT-Politik müssen noch abgewartet werden.

Immerhin wurden bei der Polizei und beim Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) zwei Großprojekte mit der Inbetriebnahme der IT-Verfahren *POLIKS* (Polizeiliches Informations- und Kommunikationssystem) für die polizeiliche Sachbearbeitung und EWW-neu (mit dem Produkt *MESO* – Meldeamt Software –) für das Einwohnerwesen abgeschlossen.

Beide Verfahren gerieten mit der Inbetriebnahme in die Schlagzeilen der Presse und auf die Tagesordnung des Innenauschusses des Berliner Abgeordnetenhauses. Es gab erhebliche Anfangsschwierigkeiten, die insbesondere bei POLIKS zu Einbußen der Verfügbarkeit und damit zu Störungen der Aufgabenerfüllung bei der Berliner Polizei führten. Leider ist es nicht ungewöhnlich, dass es bei der Einführung neuer IT-Systeme zu solchen Problemen kommt. POLIKS als völlige Neuentwicklung musste sich erst einmal im Echtbetrieb bewähren, bei dem es zu einer Vielzahl von gleichzeitigen Zugriffen durch in der Regel noch nicht mit dem System vertraute Sachbearbeiter kommt. Die Kinderkrankheiten eines neu entwickelten Programms im Zusammenspiel mit Bedienungsproblemen führten zu erheblichen Verfügbarkeitsproblemen. Mit dem Ausbügeln der Softwarefehler und sich aufbauenden Routine der Mitarbeiter sollten die Probleme seltener werden.

Ähnliches gilt für *EWW-neu*, welches zwar auf einem bundesweit erprobten und bewährten Produkt aufbaut, dessen Anpassung an eine Stadt von der Größe Berlins und deren besondere Anforderungen dennoch zu Anfangsschwierigkeiten führten. Die auch hier noch fehlende Vertrautheit der Mitarbeiter mit dem neuen Verfahren führte zur Verlängerung der Wartezeiten in den Bürgerämtern. Mittlerweile scheint die Gewöhnungsphase weitgehend abgeschlossen zu sein.

IT-Politik in der Berliner Landesverwaltung

Über die neuen gesetzlichen und verwaltungsorganisatorischen Rahmenbedingungen der Entscheidungsfindung und Organisation der Datenverarbeitung in der Berliner Verwaltung haben wir in den letzten beiden Jahren bereits berichtet. Der frühere Landesbetrieb für Informationstechnik (LIT) wurde per Gesetz zur Anstalt öffentlichen Rechts und genießt so größere Unabhängigkeit vom haushalts- und verwaltungsrechtlichen Korsett, das eine normale Behörde, aber auch ein auf Grundlage der Landeshaushaltsordnung operierender Landesbetrieb zu tragen hat. Die Zuständigkeit des Senats für die Regelungen im Bereich der Informationstechnik wurde durch die Anpassung des Allgemeinen Zuständigkeitsgesetzes erweitert und neue Verwaltungsvorschriften für die

Steuerung des IT-Einsatzes in der Berliner Verwaltung (VV IT-Steuerung) ordneten die Entscheidungs- und Beratungsstrukturen neu.

In einer Konferenz wurde Ende März 2005 festgelegt, dass sich die künftige IT-Politik des Landes an der Verfolgung von fünf Handlungsfeldern zu orientieren habe:

- *Dienstleister ITDZ*: Die Berliner Verwaltungen benötigen das IT-Dienstleistungszentrum als leistungsfähigen und zuverlässigen Partner bei der Durchführung von IT-Projekten.

- *Basisdienste E-Government*: Es sind Basisdienste zu entwickeln und einzurichten, damit die technischen und organisatorischen Voraussetzungen für eine landesweit koordinierte Umsetzung des E-Government geschaffen werden.

- *Betriebskonzepte/Betriebssysteme*: Wegen der steigenden Anforderungen an die PC-Arbeitsplätze und der knapper werdenden finanziellen Ressourcen werden neue Betriebskonzepte bzw. Betriebssysteme benötigt.

- *Fachverfahren:* Die Planung und Einführung neuer Fachverfahren in der Verwaltung sollen zur Vermeidung von Reibungsverlusten (z. B. durch Doppelarbeit) und Folgekosten verstärkt koordiniert werden.

- *IT-Kompetenzzentrum und IT-Regelwerk*: Das IT-Kompetenzzentrum in der Senatsverwaltung für Inneres unterstützt die Verwaltungen bei der Umsetzung des IT-Regelwerks (VV IT-Steuerung) und entwickelt es weiter.

Im Rahmen dieser strategischen Zielsetzungen wurden neun prioritäre Projekte definiert und angestoßen:

- Es wird eine *Landesvereinbarung zu Dienstleistungen im Bereich der Sprach- und Telekommunikation* erarbeitet und zwischen dem IT-Kompetenzzentrum und dem ITDZ geschlossen. Die Landesvereinbarung regelt das Angebot und die Preisgestaltung für die in diesem Bereich zu erbringenden Dienstleistungen des ITDZ für die Berliner Verwaltung. Die Nutzung der Dienstleistungen soll landesweit verbindlich gemacht werden und die zu erbringende Qualität und die Preise sollen ebenfalls landesweit transparent gemacht und akzeptiert werden. Zu den Dienstleistungen des ITDZ gehören auch spezielle Angeboten wie das Interne Telefonverzeichnis der Berliner Verwaltung und das in der Entwicklung begriffene Berlin-Telefon. Bei dem Berlin-Telefon handelt es sich um ein zentrales Call-Center der Berliner Verwaltung, welches zum zentralen

Ansprechpartner der Verwaltungskunden werden soll.

- Das Projekt *ProBetrieb* bildet den Schwerpunkt bei der Verfolgung des Handlungsfeldes Betriebskonzepte/Betriebssysteme. Die Prioritäten liegen dabei im Abschluss eines Landesvertrages mit der Firma Microsoft zum Einsatz ihrer Betriebssysteme, in der Migration zu neueren Versionen dieser Betriebssysteme, in der Erprobung und Verbreitung von Open Source Software wie LINUX sowie in der Einführung neuer wirtschaftlicherer und sichererer Betriebsformen, zu denen insbesondere Terminalserver-Anwendungen gehören, die bereits in einigen Verwaltungen realisiert worden sind[32].

- Das Projekt *ProForm* dient der Fortentwicklung eines einheitlichen und interaktiven Formularservices als wesentlichen Bausteins der E-Government-Dienste. Er soll über alle Vertriebswege für die Kunden (Bürger, Unternehmen) und Berliner Behörden erreichbar sein.

- Mit dem Projekt *ProOutput* soll ebenfalls ein Basisdienst für das E-Government geschaffen werden. Dabei geht es um die abgestimmte und einheitliche Organisation der Ergebnispräsentation (Output-Management) der E-Government-Angebote und um die Einrichtung zentraler Druck- und Versanddienste im ITDZ (Druckrechenzentrum) für die diversen Fachverfahren.

- Die *Virtuelle Poststelle* soll weitgehend automatisiert den elektronischen Zugang zur Verwaltung ermöglichen. Dabei sind hohe Anforderungen des Datenschutzes, der IT-Sicherheit und der Rechtsverbindlichkeit zu erfüllen. Kryptographische Verfahren zur Verschlüsselung, zur digitalen Signatur und zur Dokumentation von Zeitpunkten (Zeitstempel) sollen dies ermöglichen. Auch die Virtuelle Poststelle wird eine Dienstleistung des ITDZ sein.

- Mit dem Projekt *SIDok* wird ein ursprünglich für die Senatskanzlei gedachtes Projekt eines Senatsinformations- und Dokumentationssytems zur Verbesserung der Geschäftsprozesse landesweit aufgelegt. Grundlage dafür ist ein Document Management System (DMS).

- Mit der Ablösung der alten Richtlinien für die Organisation der IT-Projekte des Landes durch neue *IT-Organisationsgrundsätze* sollen die Rollen in den Projekten und bei der Durchführung der Datenverarbeitung, die dabei stattfindenden Prozesse und

32 vgl. auch 2.1

Beziehungen neu beschrieben werden.

- Es sollen *Standards und Normen* für die Einführung von IT-Verfahren entwickelt und verbindlich gemacht worden. Der Ansatz besteht dabei zunächst in der Präzisierung des seit längerem bestehenden Warenkorbs, der jene IT-Produkte enthält, die bevorzugt in der Berliner Verwaltung eingesetzt werden sollen und die das ITDZ anbieten kann.

- Da alles ohne Geld nicht geht, befasst sich schließlich das Projekt zur Festlegung eines *Finanzierungskonzepts* mit der Frage, wie die Umsetzung der zentralen Projekte finanziert werden soll. Dabei geht es um die Umlegung der Kosten auf die Verwaltungen, die den Nutzen aus den Projekten ziehen.

Neben den neu angetretenen Funktionsträgern und Verwaltungsgremien zur Verfolgung einer effizienten IT-Politik zur Bereitstellung von Bürgerdiensten in einer modernen Verwaltung hat auch das Abgeordnetenhaus von Berlin dem Senat seine Forderungen an eine künftige IT-Politik formuliert. In den Auflagen zum Haushaltsplan 2006/2007 wird dem Senat u. a. aufgetragen, eine IT-Strategie vorzulegen, in der Maßnahmen vorzusehen sind, die die uneingeschränkte Verwendung von Open-Source-Betriebssystemen und -Anwendungsprogrammen ermöglichen; bei Softwarebeschaffungen sind zudem offene Schnittstellen und Dokumentenformate anstelle von herstellerabhängigen Quasistandards zugrunde zu legen.

IT-Sicherheit in Berlin

Sicherheit im *Berliner Landesnetz*

Zum Berliner Landesnetz wurden Maßnahmen zur IT-Sicherheit und zum Datenschutz weiter diskutiert. Beispielsweise wurde klargestellt, dass das im Jahresbericht 2004[33] beschriebene Verfahren „HTTPS-Scan“ im Grenznetz des Berliner Landesnetzes zum Schutz von Viren und Würmern im verschlüsselten Webverkehr nur unter den dort genannten Umständen und Bedingungen und nur in klar festzulegenden engen Grenzen zulässig ist. Derzeit wird analysiert, für welche Datenübertragungen ein HTTPS-Scan stattfinden kann und welche Fachverfahren von einer Anwendung des Scan-Verfahrens ausgenommen werden.

Ein weiterer Gegenstand der Diskussionen waren die Probleme, die durch die weitgehenden Zugriffsrechte der Administratoren im ITDZ im „E-Mail-Telefonbuch“ (Active Directory – AD) der Berliner Verwaltungen für einzelne Behörden entstehen. Ein Lösungsansatz liegt vor und wird von uns im Rahmen der weiteren Entwicklung datenschutzrechtlich und sicherheitstechnisch

33 JB 2004, 4.8.3

beurteilt.

IT-Sicherheitskonzepte

Die bereits im Jahre 2004 bekannt gewordenen Ergebnisse der Untersuchung des Berliner Rechnungshofes zum Bestand und zur Qualität der in den Berliner Behörden bestehenden Sicherheitskonzepte haben erfreulicherweise zum Abbau der Lethargie geführt, die es bis dahin zur Frage der Entwicklung und Umsetzung von Sicherheitskonzepten gegeben hat. Die Lethargie beruhte darauf, dass zwar die Notwendigkeit von Sicherheitskonzepten zumindest in den Bereichen des IT-Managements unbestritten war, dass jedoch die Bereitstellung der dafür notwendigen Mittel häufig an anderen Prioritäten scheiterte, obwohl eindeutige gesetzliche Regelungen (§ 5 Abs. 3 Satz 1 BlnDSG, seit 2001) und Verwaltungsvorschriften (IT-Sicherheits-richtlinie des Landes Berlin, seit 1999) dies unmissverständlich verlangten. Dies ist zumindest im Bereich der Hauptverwaltung und ihren nachgeordneten Behörden erkennbar anders geworden, denn die Zahl uns bekannt gegebener Sicherheitskonzepte zu neuen IT-Verfahren ist deutlich angestiegen. Die Qualität der Konzepte ist ebenfalls deutlich gestiegen, seit die Einsicht gewachsen ist, dass die Erstellung solcher Konzepte professionellen Sachverstandes bedarf, der von spezialisierten Beratungsunternehmen bereitgestellt wird, solange die Verwaltung dort selbst nicht genügend Know-how aufweisen kann. Zwar gab es auch dort Ausnahmen im Einzelfall, aber in der Regel waren die Sicherheitskonzepte methodisch nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellt worden und daher plausibel und hinsichtlich der Risikoanalyse offenkundig vollständig.

Die gesetzliche Regelung in § 5 Abs. 3 Satz 1 BlnDSG ist „vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung“ zu beachten und verlangt, die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Die Frage steht insbesondere dann an, wenn IT-Verfahren neu eingeführt oder wesentlich geändert werden sollen. Bei den gesetzlich geforderten Sicherheitskonzepten handelt es sich folgerichtig um verfahrensspezifische Sicherheitskonzepte im Sinne der IT-Sicherheitsrichtlinie. Verfahrens-spezifische Sicherheitskonzepte befassen sich mit

- den vom Verfahren aufgeworfenen IT-Sicherheitsfragen,
- dem Schutzbedarf der zu verarbeitenden Daten in Bezug auf die in § 5 Abs. 2 BlnDSG genannten Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz,
- den vorhandenen Sicherheitsfunktionalitäten, z. B. zusätzliche

Authentisierungsverfahren für die Benutzer, verfahrensspezifische Verschlüsselungen, Schnittstellen zu anderen Verfahren,

- den besonderen Einsatzumgebungen der Anwendung (z. B. Räumlichkeiten, Art ihrer Nutzung, Qualifikation der Benutzer usw.)

und behandeln Sicherheitsfragen im Zusammenhang mit ggf. zu verwendender verfahrensspezifischer Soft- und Hardware, die ansonsten nicht Teil der vom Verfahren unabhängigen IT-Infrastruktur der anwendenden Stelle sind.

Nutzt das IT-Verfahren als eines von mehreren die IT-Infrastruktur der Behörde, so profitiert es auch von Maßnahmen zur Herstellung der IT-Sicherheit, die für die behördliche IT-Infrastruktur bereits getroffen worden sind. Nach der IT-Sicherheitsrichtlinie sind diese Maßnahmen in einem behördenspezifischen Sicherheitskonzept zu ermitteln, festzulegen und umzusetzen. Anders als bei den verfahrensspezifischen Sicherheitskonzepten, die im Berliner Datenschutzgesetz verlangt werden, kann eine Verbesserung der Lage in der Berliner Verwaltung bei den behördenbezogenen Konzepten nicht konstatiert werden. Behördenspezifische Sicherheitskonzepte von hinreichender Qualität sind uns bisher nur sehr sporadisch bekannt geworden, eine positive Entwicklung ist nicht zu erkennen.

Das Fehlen behördlicher Sicherheitskonzepte wirkt sich auf die Sicherheit der IT-Verfahren aus, denn deren Sicherheitskonzepte sind ja auch von der Sicherheit der behördlichen IT-Infrastruktur, dem sog. Behördennetz oder – in den Bezirken – Rathausnetz, abhängig.

Aus diesem Grunde ist die häufig im Zusammenhang mit der Einführung neuer Verfahren vertretene Auffassung abwegig, dass man sich mit der Sicherheitslage der behördlichen Infrastruktur beim verfahrensspezifischen Sicherheitskonzept nicht befassen müsse, da die Zuständigkeit dafür nicht beim Verfahrensverantwortlichen, sondern bei den Verantwortlichen für die IT-Infrastruktur, meist der für die Informationstechnik verantwortlichen zentralen Stelle der Behörden liegt. Eine solche Haltung hätte zur Konsequenz, dass man zwar ein verfahrensspezifisches IT-Sicherheitskonzept, dennoch aber keine belegbare IT-Sicherheit hätte.

Wenn eine Behörde kein behördenspezifisches Sicherheitskonzept hat, muss ein verfahrensspezifisches Sicherheitskonzept auch die vom Verfahren unabhängige Infrastruktur, die jedoch vom Verfahren benutzt wird, in der *Risikoanalyse* und bei der Auswahl der treffenden Maßnahmen einbeziehen. Das Berliner Datenschutzgesetz verlangt nämlich nicht, wohlmeinende Papiere mit Risikoanalysen und Sicherheitskonzepten zu schreiben, es verlangt vielmehr die Gewährleistung von effektiver IT-Sicherheit.

Es gibt jedoch Anlass zur Hoffnung, dass es auch bei den behördenspezifischen Sicherheitskonzepten in der Zukunft Fortschritte geben wird. Grundlage dafür ist der vorläufige erfolgreiche Abschluss der Arbeiten am *Modellsicherheitskonzept* durch die dafür eingerichtete Arbeitsgruppe des IT-Koordinierungsgremiums. Das Modellsicherheitskonzept wurde zu Beginn des Jahres mit der Version 0.4 bekannt gemacht und zur Anwendung empfohlen. Ende des Jahres beendete die Arbeitsgruppe ihre Tätigkeit mit der Version 1.0. Die Anpassung an neuere Entwicklungen soll dann von der ständigen Arbeitsgruppe IT-Sicherheit geleistet werden.

Das Modellsicherheitskonzept wurde auf der Grundlage des *IT-Grundschutzhandbuchs* des Bundesamtes für Sicherheit in der Informationstechnik entwickelt, indem es die in Berlin bereits getroffenen Maßnahmen aus dem Sicherheitskonzept für die zentrale Infrastruktur (Berliner Landesnetz, ITDZ-Sicherheitsrechenzentrum, Grenznetz zwischen Landesnetz und Internet) und die damit verknüpften zentralen Sicherheitsdienstleistungen sowie das der IT-Sicherheit dienende IT-Regelwerk (vor allem die IT-Sicherheitsrichtlinie) berücksichtigt und im Grundschutzhandbuch behandelte Komponenten ausblendet, sofern sie in der Berliner Verwaltung nicht eingesetzt werden. Im Ergebnis kann das Modellsicherheitskonzept als das auf Berliner Verhältnisse heruntergebrochene Grundschutzhandbuch angesehen werden. Ziel ist dabei, den Berliner Behörden zu ermöglichen, aus eigener Kraft behördenspezifische Sicherheitskonzepte fachgerecht erstellen zu können. Der Aufwand wird dabei von den kostenintensiven Beauftragungen externer Unternehmen auf den personellen Einsatz eigener Kräfte verlagert. Es bleibt abzuwarten, ob die Behörden angesichts des Personalabbaus dazu bereit sein werden.

Aktuelle IT-Projekte des Landes

Zu den eingangs erwähnten Großprojekten POLIKS und EWW-neu im Sicherheits- und Ordnungsbereich des Landes gesellte sich eine Reihe weiterer neuer IT-Projekte in den unterschiedlichen Verwaltungsbereichen.

Bereits seit einigen Jahren läuft das Projekt *Integrierte Software Berliner Jugendhilfe (ISBJ),* welches verschiedene Anwendungen aus dem Jugendbereich (Kindertagesstätten, Bundeserziehungsgeld, Hilfe zur Erziehung, Zentrale Vormundschafts- und Unterhaltsvorschusskasse) unter einem Dach vereinigt und mit übergeordneten Komponenten ergänzt. Zu diesen zentralen Komponenten gehört eine Personenstammverwaltung, die regelmäßig mit den Daten des Melderegisters abgeglichen wird. Hier wird es darauf ankommen, auf Landesebene zu Rechtsgrundlagen für die Führung der zentralen Datei und für den Online-Zugriff auf das Melderegister zu kommen.

Die Gesundheitsämter der Bezirke werden in der nächsten Zeit mit neuen Fachverfahren ausgestattet. Gegenstand einer datenschutzrechtlichen Kontrolle war dabei das Verfahren *SpDI32* zur Unterstützung der Abläufe in den *Sozialpsychiatrischen Diensten*. Über das Ergebnis der Kontrolle berichten wir im Abschnitt 4.9.2. Auf der Grundlage von SpDI32 wurden weitere Verfahren für die *Kinder- und Jugendpsychiatrischen Dienste (KiPsI32)* und für die *Beratungsstellen für Behinderte und Chronisch Kranke (BfBI32)* entwickelt. Allen diesen Verfahren gemeinsam ist, dass sie Daten von außerordentlichem Schutzbedarf verarbeiten und es damit darauf ankommt, dass gut umgesetzte Sicherheitskonzepte die Vertraulichkeit der Daten gewährleisten. Problematisiert werden musste die Frage nach der Einbindung eines externen Dienstleisters für die Programmpflege und -wartung bei diesen Verfahren. Mit den Grundsätzen der ärztlichen Schweigepflicht wäre es unvereinbar, wenn Dritte ohne direkte Aufsicht ärztlichen Personals Zugang zu solchen Daten bekämen.

Nachdem die Freie Universität Berlin davon Abstand nahm, für die Prüfungsverwaltung das weit verbreitete Programm HIS-POS der im öffentlichen Besitz befindlichen Hochschul-Informations-System GmbH zum Einsatz zu bringen, weil es als nicht geeignet eingeschätzt wurde, die besonderen Anforderungen von prüfungsintensiven Master- und Bachelor-Studiengängen zu erfüllen, wurde in Zusammenarbeit mit der SAP AG in kurzer Zeit ein Programm *Campus Management* entwickelt und eingesetzt. Die FU hatte Datenschutz- und IT-Sicherheitsaspekte zu einem Schwerpunkt des Projekts gemacht. Dennoch löste die kurzfristige Inbetriebsetzung Aufregung bei den Betroffenen aus, die „gläserne“ Studierende befürchteten. In der Tat hinterlassen die Studierenden erheblich mehr Spuren als früher in den alten Studiengängen. Dies ist aber nicht dem IT-System zuzuschreiben, sondern den neuen Studiengängen und Prüfungsanforderungen, mit denen die Anzahl prüfungsrelevanter und daher zu registrierender

Leistungen etwa verzehnfacht worden ist.

Die weiter oben beschriebene IT-Politik des Landes hat hauptsächlich die Entwicklung interaktiver Bürgerdienste im Rahmen des E-Government im Auge. Als eines der ersten konkreten Projekte im Rahmen der neuen Prioritätssetzungen wurde uns das Projekt *Berlin-Telefon* präsentiert. Dabei geht es um die Einführung eines großen Call-Centers der Verwaltung, das zentral im ITDZ betrieben werden soll. Die Bürger sollen die Verwaltung in Zukunft über eine einheitliche Telefonnummer erreichen können. Sofern das *Call-Center* die Informationswünsche der Bürger nicht unmittelbar befriedigen kann, wird die Verbindung zu dezentralen „Front Offices“ in den Behörden hergestellt, die die Fragen konkreter behandeln und bei Bedarf auch zu den Sachbearbeitern durchstellen können. Daten der Bürger werden in diesem Kontext nur dann gespeichert, wenn der gewünschte Kontakt nicht hergestellt werden kann und daher ein Rückruf oder eine Remail vereinbart werden muss.

3. Schwerpunkte im Berichtsjahr

3.1 Videoüberwachung in öffentlichen Verkehrsmitteln und Wohnanlagen

Der *öffentliche Personennahverkehr* (ÖPNV) wird nach den Vorstellungen der Verkehrsplaner in naher Zukunft stark durch vernetzte Informationstechnik geprägt sein. Ein wesentlicher Aspekt aus Sicht des Datenschutzes ist dabei der Einsatz der Videotechnik. Seit Jahren wird diese Technik zu verschiedenen Zwecken sowohl bei der Deutschen Bahn als auch bei den Berliner Verkehrsbetrieben (BVG) in U-Bahnen, Bussen und Straßenbahnen eingesetzt. Zum einen sollen damit der Verkehrsfluss und die Verkehrs-regulierung optimiert werden (z. B. zur Unterstützung der Zugabfertigung), zum anderen soll die Videoüberwachung den Sicherheitsstandard für die Fahrgäste verbessern und Belästigungen, Bedrohungen und Gefährdungen von Personen im Bahnbereich vorbeugen. Des Weiteren soll die Überwachung zum Schutz der Anlagen und Fahrzeuge vor missbräuchlicher Benutzung, Beschädigung oder Diebstahl dienen.

3-S-Konzept der Deutsche Bahn AG (DB AG)

Mit ihrem bereits 1995 konzipierten 3-S-Programm möchte die DB AG Service, Sicherheit und Sauberkeit im Bahnbereich verbessern. Zu diesem Zweck wurden die großen Bahnhöfe mit Videoanlagen ausgerüstet, die über ferngesteuerte *Speed-Dome-Kameras* verfügen, sich automatisch auf die verschiedenen Lichtsituationen bei Tag und Nacht einstellen und weite Bereiche des Bahnhofs erfassen. Die Mitarbeiter der Bahn in den 3-S-Zentralen haben den Bahnhofsbereich über mehrere Monitore im Blick und stehen mittels modernster Kommunikationstechnik mit bahneigenen Stellen, aber auch mit der Bundespolizei (früher: Bahnpolizei) in Verbindung. Die Aufgaben der 3-S-Zentralen umfassen:

- Abwicklung des Betriebsprogramms
- Sicherstellen von Service, Sicherheit und Sauberkeit
- Sicherstellen des Notfall- und Securitymanagements
- Sicherstellen der Kundeninformation (Reiseinformation)
- Sicherstellen der Verkehrssicherungspflichten

Die DB AG und die Bundespolizeidirektion werden einen Vertrag über die Nutzung der optisch-elektronischen Einrichtungen (*Videoüberwachung, -aufzeichnung*) in den Bahnhöfen der DB AG durch die Bundespolizei abschließen. Die Aufzeichnung soll bedingt durch diverse Ereignisse

(Verschärfung der allgemeinen Sicherheitslage nach dem 11. September 2001 oder dem Bombenfund im Dresdner Hauptbahnhof im Juni 2003) nicht mehr anlassbezogen, sondern kontinuierlich erfolgen. Allerdings beschränkt sich die DB AG darauf, soweit sie eigene Zwecke im Rahmen des 3-S-Programms verfolgt, die Videobilder zu beobachten und im Anschluss daran Maßnahmen zu ergreifen, wie etwa Reinigungspersonal anzufordern oder eine schnelle Unterstützung für einen Behinderten sicherzustellen.

Die Aufzeichnung der Videoaufnahmen durch die DB AG erfolgt ausschließlich im Interesse und im Auftrag der *Bundespolizei,* nicht jedoch zur Sicherstellung des 3-S-Konzepts. In dem Vertrag verpflichtet sich die DB AG, die aufgezeichneten Daten nicht für eigene Zwecke zu verwenden. Diese Verpflichtung wird dadurch sichergestellt, indem technisch ausgeschlossen wird, dass Bahnmitarbeiter auf gespeicherte Videobilder zugreifen. Ein Nutzungsrecht besteht auch dann nicht, wenn die DB AG, etwa zur Durchsetzung von Schadensersatzansprüchen, ein wirtschaftliches Interesse an den gespeicherten Daten hat. Eine Datenübermittlung von der Bundespolizei an die DB AG ist danach nur unter den engen gesetzlichen Vorgaben des § 32 Abs. 4 und 5 Bundespolizeigesetz (BPolG) möglich.

Da die DB AG die Videoaufzeichnungen als Auftragnehmer für die Bundespolizei erstellt, richtet sich die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung nach den für den Auftraggeber geltenden Gesetzen, insbesondere nach dem Bundespolizeigesetz (vgl. § 27 Abs. 1 Nr. 2 BPolG). Problematisch könnte sein, ob die Aufzeichnung von Videoaufnahmen, die sich auf die Bilder beziehen, die die DB AG im Rahmen ihres 3-S-Konzepts mittels optisch-elektronischer Einrichtungen beobachtet, durch diese Norm gerechtfertigt ist, da das 3-S-Konzept gerade auch Videobeobachtungen von Personen enthält, die keiner Straftat verdächtigt werden (z. B. zoomen von Behinderten, bei denen sichergestellt werden soll, dass von der Bahnhofsmission rechtzeitig Hilfestellung geleistet wird). Da die Bundespolizei zur Verwendung selbständiger Bildaufnahmen und Bildaufzeichnungsgeräte in Verkehrsanlagen und öffentlichen Verkehrsmitteln oder in unmittelbarer Nähe ermächtigt ist, eine Auswertung der Aufzeichnungen nur anlassbezogen erfolgen soll und die Bundespolizei verpflichtet ist, Videoaufzeichnungen unverzüglich zu vernichten, wenn sie nicht mehr zur Abwehr gegenwärtiger Gefahren oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden, hat der für die Bundespolizei zuständige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit keine Bedenken gegen das Verfahren.

Videoüberwachung bei der BVG

In jeder *Videoüberwachung* (*Videobeobachtung* und noch intensiver bei der *Videoaufzeichnung*) von Personen liegt ein Eingriff in deren Recht auf informationelle Selbstbestimmung wie auch in das Grundrecht auf unbeobachtete Freizügigkeit (Art. 11 GG) vor. Dieser Eingriff ist nicht von vornherein unzulässig, bedarf aber der Rechtfertigung und muss dem Verhältnismäßigkeitsgrundsatz genügen. Deshalb hat die BVG in Abstimmung mit uns bereits seit Ende der 90er Jahre Videokameras auf allen U-Bahnhöfen installiert, die eine permanente Beobachtung der Bahnhöfe ermöglichen. Eine Aufzeichnung von Bildern findet bislang aber nur anlassbezogen statt, etwa wenn auf dem Monitor in der Leitstelle eine Straftat beobachtet oder die Notrufsäule auf dem Bahnsteig betätigt wird. In den modernen U-Bahnzügen der Baureihe H (ohne Unterteilung zwischen den Waggons) und den Straßenbahnen findet dagegen eine anlassunabhängige, 24-stündige Aufzeichnung der Bilder statt. Falls nach 24 Stunden kein Vorfall gemeldet wird, sollen die Bilder gelöscht werden. Dieses Verfahren halten wir datenschutz-rechtlich wegen der Unübersichtlichkeit der U- und Straßenbahnzüge für hinnehmbar.

Anders ist die Situation in Bussen der BVG, wo der Fahrer auf einem Monitor verschiedene Bilder von den im Bus angebrachten Kameras angezeigt bekommt. Die Kameras zeichnen Bilder in einem sechsminütigen *Ringspeicher* auf, und nur wenn der Fahrer aus gegebenem Anlass einen Aufzeichnungsknopf drückt, werden alle weiteren Bilder – einschließlich der sechs Minuten vor dem Knopfdruck – aufgezeichnet, bis die Aufnahme wieder gestoppt wird. Dieses Verfahren hat die BVG – ebenfalls in Abstimmung mit uns – 1999 eingeführt und seitdem praktiziert, ohne dass sich nach unserem Kenntnisstand Fahrgäste oder BVG-Mitarbeiter darüber beschwert hätten.

Erst im Dezember 2005 kam es nach der tödlichen *Messerattacke* eines Jugendlichen in einem BVG-Bus zu einer heftigen öffentlichen Debatte darüber, ob dieses Verfahren zu ändern ist. Die Diskussion darüber war zum Ende des Berichtzeitraums noch nicht abgeschlossen.

Um das subjektive Sicherheitsgefühl ihrer Fahrgäste zu erhöhen und die Strafverfolgung für die Ermittlungsbehörden zu erleichtern, plant die BVG bereits seit längerem, die auf U-Bahnhöfen mit Videokameras gemachten Bilder aufzuzeichnen. Die günstigen Positionen der bereits zahlreich installierten Kameras bieten nach Aussage der BVG dabei eine von mehreren Voraussetzungen für eine erfolgreiche Strafverfolgung. In diesem Zusammenhang haben seit Mai 2005 mehrere Gespräche zwischen dem Vorstand der BVG und uns über die Aufrüstung der vorhandenen Videoeinrichtungen mit Speicherkapazitäten für mindestens ein Jahr stattgefunden.

Im Juli 2005 stellte uns die BVG ihr *Pilotprojekt „24 Stunden Videoaufzeichnung auf drei U-Bahnlinien“* vor. Dieses Projekt soll ab März 2006 und damit auch während der Fußball-WM stattfinden. Die vorgesehenen U-Bahnlinien weisen ein besonders hohes Verkehrsaufkommen und eine entsprechend hohe Kriminalitätsbelastung auf. Die BVG will uns sowohl nach den ersten sechs Monaten als auch nach Beendigung des Projekts einen Bericht über ihre praktischen Erfahrungen mit der *Videoaufzeichnung* vorlegen. Aus diesem Bericht soll sich u. a. auch die Zahl der Fälle ergeben, in denen Aufzeichnungen längerfristig zu bestimmten Zwecken vorgehalten wurden. Rechtsgrundlage für dieses Pilotprojekt wie für jede Form der Videoüberwachung ist § 31 b des Berliner Datenschutzgesetzes (BlnDSG), der auf die BVG als öffentliche Stelle des Landes Berlin anzuwenden ist.

Danach ist die Videoüberwachung öffentlich-zugänglicher Räume nur zulässig, soweit sie zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen (am Ausschluss der Überwachung) überwiegen. Der Umstand der Beobachtung und die Daten verarbeitende Stelle sind durch Hinweisschilder erkennbar zu machen.

Unabhängig von den Ergebnissen des Pilotprojekts lässt sich mit dieser Vorschrift keine flächendeckende permanente Videoaufzeichnung auf allen Berliner U-Bahnhöfen rechtfertigen. Denn es gehört nicht zu den Aufgaben der BVG, die Strafverfolgung oder die Gefahrenabwehr zu erleichtern. Auch die Wahrnehmung des *Hausrechts* rechtfertigt Videoaufzeichnungen nur, soweit dies angesichts der Gegebenheiten auf bestimmten U-Bahnhöfen erforderlich ist, nicht aber flächendeckend im gesamten U-Bahnnetz.

Zwar können Aufnahmen, die die BVG im Rahmen ihres Hausrechts für eigene Zwecke macht, bei Bedarf im Einzelfall auch den Strafverfolgungsbehörden zugänglich gemacht werden. Soll die BVG aber vorsorglich routinemäßige Videoaufzeichnungen als Beweismittel für künftige Straftaten anfertigen, so ließe sich dies nicht einmal durch eine Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes legitimieren. Denn nach der Entscheidung des Bundesverfassungsgerichts zum Niedersächsischen Polizeigesetz[34] liegt die Gesetzgebungskompetenz für Maßnahmen zur Vorsorge für die Verfolgung von Straftaten allein beim Bund.

Für das geplante Pilotprojekt legte uns die BVG im November 2005 einen Entwurf ihres Datenschutzkonzepts vor. Darin werden die technischen und organisatorischen Rahmenbedingungen der Videolangzeitarchivierung für die Dauer von 24 Stunden erläutert. Die Videoaufnahmen werden demnach dezentral auf Festplatten, die in die bereits vorhandenen Rechner

34 Urteil v. 27. Juli 2005 – 1 BvR 668/04

eingebaut werden sollen, archiviert und erst im Ereignisfall oder bei Anfragen der Ermittlungsbehörden zentral an einem Auswertungsplatz in der BVG-Zentrale ausgewertet. Die Berechtigung zum Auslesen und Überspielen der gespeicherten Videodaten ist personenbezogen und auf maximal sieben ausgewiesene zugangsberechtigte BVG-Mitarbeiter beschränkt. Jedem dieser Mitarbeiter ist ein spezielles Anmeldekennwort und ein spezifischer Nutzername zugeordnet. Alle berechtigten Personen sind gemäß § 8 BlnDSG vertraglich verpflichtet worden, das Datengeheimnis zu wahren, wonach es ihnen untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Diese Pflichten bestehen auch nach Beendigung ihrer Tätigkeiten fort. Nach 24 Stunden erfolgt eine automatische Überschreibung der Aufzeichnungen. Nur das anlassbezogen für die Strafverfolgung relevante Videomaterial wird auf einen Datenträger (DVD) überspielt und dabei entschlüsselt. Der Datenträger wird anschließend den zuständigen Ermittlungsbehörden gegen Empfangsbescheinigung übergeben. Eine Auslagerung oder eine Lagerung der beschriebenen Datenträger erfolgt nicht.

Sowohl aus technischer als auch aus datenschutzrechtlicher Sicht war das erste Datenschutzkonzept für das angestrebte Pilotprojekt der BVG lückenhaft. Erst nach dem Ende des Berichtszeitraums legte die BVG ein verbessertes Datenschutzkonzept vor, das unseren Forderungen weitgehend entsprach.

Inwieweit die Videoaufzeichnung Auswirkungen auf die Sicherheit in U-Bahnhöfen und die Strafverfolgung hat, soll auf unseren Vorschlag hin innerhalb einer wissenschaftlichen Begleitung dieses Pilotprojekts untersucht werden. Experten des Zentrums Technik und Gesellschaft der Technischen Universität Berlin werden eine unabhängige externe Evaluation durchführen, die sich in folgende drei Arbeitsphasen gliedern wird:

1. *Vorfeldanalyse:* Vor Beginn der Evaluation muss der Ist-Zustand erfasst werden (Vorhermessung). Dazu wird eine Analyse der Überwachungsintensität sowie die Lokalisierung kritischer Stationen und Standorte vorgenommen. Als wesentliche Grundlage dienen Auswertungen sämtlicher vorhandener Statistiken der Polizei und BVG.

2. *Pilotprojekt:* Nach Einführung der Videoaufzeichnung wird eine Nachhermessung vorgenommen, die u. a. Fahrgastumfragen auf allen untersuchten Linien beinhaltet (z. B. Wahrnehmung des Projekts, allgemeines Sicherheitsempfinden etc.). Die Ergebnisse werden in einem Zwischenbericht dargestellt.

3. *Endauswertung:* Es erfolgt ein Vergleich zwischen Vorher- und Nachhermessung sowie eine Interviewauswertung in Bezug auf die statistische Analyse in 1.) und 2.). Ein

Abschlußbericht beendet die wissenschaftliche Begleitung des Projekts.

Ob die wissenschaftliche Begleitung des Projekts tatsächlich wie beschrieben ablaufen wird, stand zum Redaktionsschluss noch nicht fest. Erst nach Auswertung der Begleituntersuchung soll über eine mögliche Erstreckung der Videoaufzeichnung auf andere Linien entschieden werden.

Das Berliner Datenschutzgesetz ermöglicht Videoaufzeichnungen nur anlassbezogen oder – anlassunabhängig für einen begrenzten Zeitraum – bei bestimmten örtlichen Gegebenheiten.

Die beste Sicherheit im öffentlichen Personennahverkehr bieten personalbesetzte Bahnhöfe. Sichtbarer kompetenter und enger Kundenkontakt ist dabei am effektivsten und sollte in diesem Zusammenhang allen technischen Überwachungsmöglichkeiten vorgezogen werden.

Kameras in *Wohnanlagen* – die kostenlose Live-Fernsehshow

> *Einer der größten deutschen Kabelnetzbetreiber hat in zahlreichen Berliner Wohnanlagen das sog. TELECOP-System installiert, bei dem Videokameras den Eingang zu Mehrparteienhäusern permanent überwachen. Die dabei gewon-nenen Bilder werden live in das jeweilige Hauskabelnetz eingespeist. Alle Wohnungsnutzer können sich rund um die Uhr diese Bilder im eigenen Fernsehgerät als zusätzliches „Programm“ ansehen und nach Belieben aufzeichnen. Darüber beschwerten sich mehrere Bürger bei uns.*

Der Betrieb dieses Überwachungssystems verstößt gegen § 6 b Bundesdatenschutzgesetz. Öffentlich zugängliche Räume – und dazu zählen auch die genannten *Hauseingangsbereiche* – dürfen nur dann optisch-elektronisch beobachtet werden, wenn dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Zur Wahrnehmung des Hausrechts ist das System ungeeignet, da die Bilder ausschließlich in die Wohnungen der Mieter übertragen und dem Inhaber des Hausrechts für den Eingangs-bereich – dem Hauseigentümer – oder seinen Bevollmächtigten, z. B. einem Hausmeister, nicht zugänglich gemacht werden. Ob die Mieter den Eigentümer z. B. über beobachtete Sachbe-

schädigungen informieren, bleibt ihnen überlassen.

Es ist auch zweifelhaft, ob die Übertragung von Videobildern aus den Hauseingängen an alle Wohnungsnutzer der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Jedenfalls überwiegen aber schutzwürdige Interessen der Betroffenen. Denn sowohl Mieter als auch Besucher können von jeder Wohnung aus beim Betreten und Verlassen des Hauses beobachtet werden. Diese Bilder können von jedem, der Zugang zu einem Fernsehgerät in einer angeschlossenen Wohnung hat, aufgezeichnet und unbegrenzt gespeichert werden. Darin liegt nach der Rechtsprechung des *Kammergerichts* ein unzulässiger Eingriff in das Persönlichkeitsrecht der Bewohner wie auch der Besucher, die einer ständigen Überwachung ausgeliefert werden, auch wenn sie nicht die Klingel zu einer bestimmten Wohnung betätigen[35]. Diese Form der Überwachung ist auch deshalb von erheblich belastendem Gewicht, weil sie die Hauseingangsbereiche zu jeder Tages- und Nachtzeit unter Kontrolle hält und die Betroffenen ihr nicht ausweichen können[36].

Diese Interessen der Betroffenen sind grundsätzlich durch das Recht auf informationelle Selbstbestimmung wie auch durch das Recht am eigenen Bild geschützt und genießen Vorrang vor einem etwaigen Interesse der Wohnungsnutzer, die Begehung von Ordnungswidrigkeiten oder Straftaten in den jeweiligen Hauseingängen zu beobachten. Auch ein möglicher Abschreckungseffekt, mit dem die Betreiberfirma den Hauseigentümern und Mietern dieses zusätzliche „Programm“ schmackhaft machen will, besteht in Wirklichkeit nicht. Denn die Bilder werden nicht permanent von einem Angestellten des Hauseigentümers (z. B. Hausmeister) beobachtet, so dass mit einem schnellen Eingreifen bei Gesetzesverstößen nicht zu rechnen ist.

Zwar haben die Betreibergesellschaft und die Vermieter nach eigenen Angaben in einzelnen Wohnanlagen den Mietern Einverständniserklärungen oder Hinweise auf das System vorgelegt. Abgesehen davon, dass diese Einverständniserklärungen bei unseren Prüfungen teilweise nicht vorgelegt werden konnten, kommt es auf sie ebenso wenig an wie auf die in den Hauseingängen vereinzelt angebrachten Hinweisschilder. Denn Mieter könnten allenfalls für sich selbst wirksam einer Beobachtung zustimmen, nicht zu Lasten von unbekannten Besuchern. Diese wiederum können der Beobachtung nicht ausweichen, wenn sie das Haus betreten wollen.

Datenschutzrechtlich hinnehmbar ist nur eine Videoüberwachung von Hauseingängen, bei der wie bei einer *Gegensprechanlage* ein Videosignal ausschließlich in die Wohnung übermittelt wird, bei der im Hauseingang geklingelt worden ist. Diese von uns vorgeschlagene Lösung hat

35 Beschluss des Kammergerichts v. 26. Juni 2002 – 24 W 309/01
36 Urteil des Amtsgerichts Berlin-Mitte v. 18. Dezember 2003 – 16 C 427/02, vgl. dazu JB 2004, 4.8.4

das Unternehmen bisher aus Kostengründen ebenso abgelehnt wie technische Vorkehrungen, die das Aufzeichnen verhindern. Finanzielle Erwägungen rechtfertigen es aber nicht, eine Videoüberwachungsanlage zu betreiben, die mit dem Bundesdatenschutzgesetz unvereinbar ist und das Persönlichkeitsrecht der betroffenen Personen verletzt.

Die Videoüberwachung der Hauseingänge von Mehrfamilienhäusern und Wohnanlagen, bei der permanent Bilder in das *Hauskabelnetz* eingespeist und als zusätzliches „Programmangebot“ auf allen angeschlossenen Fernsehgeräten empfangen werden können, verstößt gegen das Bundesdatenschutzgesetz.

3.2 Hartz IV und kein Ende

Ein Jahr nach In-Kraft-Treten des Sozialgesetzbuches - Zweites Buch (SGB II) - Grundsicherung für Arbeitssuchende (kurz als "Hartz IV" bezeichnet), mit dem zum 1. Januar 2005 eine Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe erfolgte, sind viele der bereits zu Beginn bestehenden Datenschutzprobleme, die wir ausführlich in unserem letzten Jahresbericht dargestellt haben[37], noch immer nicht gelöst. Vielmehr sind mit der Gründung und Arbeits-aufnahme der Jobcenter, die in Berlin für die Gewährung der Leistungen nach dem SGB II zuständig sind, viele neue Probleme hinzugekommen. Auch müssen wir in unserer täglichen Praxis immer wieder feststellen, dass der Gesetzgeber es in der Eile des Gesetzgebungs-verfahrens zum SGB II versäumt hat, wesentliche datenschutzrechtliche Fragen zu regeln.

Träger der Leistungen nach dem SGB II sind die *Bundesagentur für Arbeit* und die kommunalen Träger, d. h. in Berlin die Bezirksämter. Um die Aufgaben einheitlich wahrnehmen zu können, wurde in jedem der zwölf Berliner Bezirke eine Arbeitsgemeinschaft gegründet, die den Namen Jobcenter trägt. Die Mitarbeiterinnen und Mitarbeiter der *Jobcenter* stammen sowohl aus der Bundesagentur für Arbeit als auch aus den Bezirksämtern, vor allem den bisherigen Sozial-ämtern. Während bislang der Bundesbeauftragte für den Datenschutz für die Datenschutz-kontrolle bei der Bundesagentur für Arbeit zuständig war und die Landesbeauftragten für den Datenschutz die Sozialämter kontrollierten, wirft die Kontrollzuständigkeit für die neu ge-gründeten Arbeitsgemeinschaften Fragen auf. Nach einhelliger Auffassung der Datenschutz-beauftragten des Bundes und der Länder handelt es sich bei den Arbeitsgemeinschaften um eigenverantwortlich Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der jeweiligen Landesbeauftragten für den Datenschutz unterliegen[38]. Zwar stellt die Bundesagentur

37 JB 2004, 3.1, S. 25 ff.

38 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 27./28. Oktober 2005 "Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen", vgl. Anlagenband "Dokumente zu Datenschutz und Informationsfreiheit 2005", S.

für Arbeit eine Kontrollkompetenz der Landesbeauftragten für den Datenschutz dem Grunde nach nicht in Frage, so dass diese auch nach Auffassung der Bundesagentur die richtigen Adressaten für Beschwerden zum Umgang der Arbeitsgemeinschaften mit personenbezogenen Daten sein sollen, jedoch bestreitet sie, dass die Arbeitsgemeinschaften Adressaten von Beanstandungen sein können und die Landesbeauftragten somit die festgestellten Datenschutzverstöße gegenüber den Arbeitsgemeinschaften auch ahnden können. Nach Meinung der Bundesagentur soll es hierfür jeweils der Mitwirkung des Bundesbeauftragten für den Datenschutz bedürfen. Diese Rechtsauffassung findet keine Grundlage im Gesetz. In der Praxis führt die Weigerung der Bundesagentur, die Arbeitsgemeinschaften als eigenverantwortlich Daten verarbeitende Stellen zu akzeptieren, zu einer Behinderung unserer Arbeit, die nicht hingenommen werden kann[39]. Durch die Haltung der Bundesagentur wird eine effektive Datenschutzkontrolle zu Lasten der Betroffenen erschwert. Der Gesetzgeber ist aufgerufen, im Interesse der Betroffenen in dieser Frage schnellstmöglich für Rechtsklarheit zu sorgen.

Die von der Bundesagentur für Arbeit vertretene Rechtsauffassung führt in Berlin dazu, dass bislang nicht alle Jobcenter der gemäß § 19 a Berliner Datenschutzgesetz (BlnDSG) bestehenden Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten bei Behörden und sonstigen öffentlichen Stellen nachgekommen sind. Obwohl die Vorschriften des Sozialgesetzbuches – Zehntes Buch (SGB X) die landesrechtlichen Vorschriften über die Bestellung behördlicher Datenschutzbeauftragter ausdrücklich für anwendbar erklären und ein Teil der Jobcenter bereits behördliche Datenschutzbeauftragte bestellt hat, wird die Verpflichtung zur Bestellung von einigen Jobcentern noch immer bestritten. Auch an dieser Stelle wird deutlich, wie wichtig eine gesetzgeberische Klarstellung der Zuständigkeiten ist.

Wir hatten bereits in unserem letzten Jahresbericht darüber berichtet, dass die Antragsvordrucke für die Beantragung des Arbeitslosengeldes II in weiten Teilen nicht datenschutzgerecht sind, da viele für die Antragsbearbeitung nicht erforderliche Angaben verlangt werden[40]. Die Bundesagentur für Arbeit hatte angekündigt, die Antragsvordrucke und Zusatzblätter bis zum Frühjahr 2005 zu überarbeiten. Diese Zusage wurde nicht eingehalten, so dass noch immer die datenschutzrechtlich bedenklichen Vordrucke verwendet werden. Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder ist mittlerweile eine Überarbeitung der Vordrucke und auch der *Ausfüllhinweise* erfolgt. Nur wenn die Antragsvordrucke den Betroffenen gemeinsam mit den Ausfüllhinweisen ausgehändigt werden, kann ein datenschutzgerechtes Ausfüllen der Unterlagen gewährleistet und auf diese Weise vermieden werden, dass nicht erforderliche personenbezogene Daten der Betroffenen erhoben werden[41]. Wir erwarten,

---

15

39 vgl. ebenda

40 JB 2004, 3.1, S. 25 ff.

41 vgl. Anlagenband 2005, a. a. O.

dass die Bundesagentur die überarbeiteten Vordrucke und Ausfüllhinweise den Betroffenen so schnell wie möglich zur Verfügung stellt, damit verhindert wird, dass diese in Unkenntnis ihrer Rechte weiterhin für ihren Leistungsanspruch nicht erforderliche Informationen offenbaren.

Gravierende Datenschutzmängel weist nach wie vor die Leistungs- und Berechnungssoftware für das Arbeitslosengeld II (A2LL) auf. Zwar hatten die Bundesagentur für Arbeit und das Bundesministerium für Wirtschaft und Arbeit, insbesondere auch nach der förmlichen Beanstandung des fehlenden Zugriffsrechtekonzeptes und der fehlenden Protokollierung der *Software A2LL* durch den Bundesbeauftragten für den Datenschutz[42], zugesagt, die Fehler zu beheben. Allerdings ist dies noch immer nicht erfolgt, so dass weiterhin 40.000 Mitarbeiterinnen und Mitarbeitern der Bundesagentur für Arbeit sowie der Arbeitsgemeinschaften der bundesweite und unkontrollierte Zugriff auf die Daten aller *Arbeitslosengeld II-Empfänger* möglich ist.

Während die Arbeitsgemeinschaften sich zunächst in erster Linie auf die Bearbeitung der Anträge auf Gewährung von Arbeitslosengeld II und damit auf den Leistungsbereich konzentrierten, werden wir zunehmend auch mit datenschutzrechtlichen Fragestellungen konfrontiert, die den Vermittlungsbereich betreffen. Die Arbeitsgemeinschaften bzw. von diesen in Anspruch genommene private Träger erheben Daten über die persönliche Situation der Betroffenen. Häufig werden ihnen Vordrucke vorgelegt, die eine Vielzahl von Fragen enthalten, die teilweise äußerst sensitive Bereiche betreffen. Hierzu gehören z. B. Fragen nach gesundheitlichen Einschränkungen, Vorliegen einer Sucht- oder Schuldenproblematik oder nach strafgerichtlichen Verurteilungen. Häufig müssen sich die Betroffenen auch einem sog. Profiling unterziehen. Aus datenschutzrechtlicher Sicht ist es nicht zulässig, hierzu von den Betroffenen anhand von umfangreichen Vordrucken Auskünfte über die gesamte Lebenssituation einzuholen. Vielmehr dürfen im Rahmen der Vermittlung lediglich diejenigen Daten erhoben werden, die tatsächlich für die Vermittlung im Einzelfall von Bedeutung sind. Eine Erhebung von Daten auf Vorrat ist zu vermeiden. Besonders problematisch ist die Erhebung personenbezogener Daten Dritter, z. B. über Familienangehörige, Bekannte der Betroffenen etc. Weiterhin ist es erforderlich, die Betroffenen auf die Freiwilligkeit ihrer Angaben hinzuweisen. Sofern die Arbeitsgemeinschaften für die Vermittlung die Leistungen privater Träger in Anspruch nehmen, haben sie die Einhaltung der datenschutzrechtlichen Vorgaben durch diese Stellen besonders sorgfältig zu überprüfen.

Eine besondere Brisanz bekommen die über die Betroffenen erhobenen Daten vor dem Hintergrund der Verwendung der von der Bundesagentur im gesamten Vermittlungsbereich eingesetzten *Software coArb*. Auch dieses Verfahren erlaubt einen bundesweiten lesenden Zugriff, der es ermöglicht, z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme

42 JB 2004, 3.2, S. 27 f.

einzusehen. Die damit verbundene Gefahr des Missbrauchs liegt auf der Hand. Das Verfahren coArb soll Mitte 2006 durch das *System VerBIS* abgelöst werden. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre frühzeitige Einbindung durch die Bundesagentur für Arbeit gefordert. Es muss sichergestellt werden, dass die Zugriffe regional beschränkt werden und ein detailliertes Berechtigungs- und Löschungskonzept entwickelt wird[43].

Mitte des Jahres wurde durch Presseberichte bekannt, dass die Bundesagentur ein *Call-Center* der Firma T-Systems damit beauftragt hatte, in ihrem Namen telefonische Befragungen von Arbeitslosengeld II-Beziehern durchzuführen. Ziel sollte eine Aktualisierung des bei der Bundesagentur gespeicherten Datenbestandes über die Betroffenen sein, um weitere Vermittlungsaktivitäten vorzubereiten. Allerdings wurde der Bundesbeauftragte für den Datenschutz im Vorfeld nicht über die geplante Telefonaktion informiert. Dieses hatte zur Folge, dass bei der *Telefonbefragung*, in deren Rahmen besonders schutzwürdige Sozialdaten erhoben wurden, wesentliche Datenschutzgrundsätze keine Beachtung fanden. Der Bundesbeauftragte für den Datenschutz hat die Telefonaktion deswegen auch scharf kritisiert und die Bundesagentur zur Beendigung der Aktion aufgerufen. Datenschutzrechtlich inakzeptabel war es insbesondere, dass die Betroffenen vorab nicht schriftlich über die geplante Aktion informiert wurden. Das ist deshalb von Bedeutung, weil zum einen jeder unangekündigte Telefonanruf einen Einbruch in die Privatsphäre darstellt und zum anderen die angerufene Person keine Möglichkeit zur Überprüfung hat, ob der Anrufer tatsächlich der ist, der er vorgibt zu sein, und ob er auftragsgemäß handelt. Wie sich aus den auch an uns gerichteten Eingaben ergab, wurde es bei diesen überfallartigen Telefonanrufen offenbar häufig versäumt, die Betroffenen auf die Freiwilligkeit ihrer Angaben hinzuweisen. Stattdessen wurden den Angerufenen teilweise Leistungskürzungen angedroht.

Im Oktober des Jahres wurde in zahlreichen Presseberichten der Eindruck erweckt, Empfängerinnen und Empfänger von Arbeitslosengeld II würden in hohem Maße Sozialbetrug begehen. Die Bundesagentur stützte sich zur Begründung auf die unangekündigte Telefonaktion. Erklärtes Ziel dieser Befragung war die Aktualisierung des Datenbestandes, nicht jedoch die Bekämpfung etwaigen *Leistungsmissbrauchs*. Von der Bundesagentur für Arbeit und dem ehemaligen Bundeswirtschaftsminister wurde allerdings in der Presse ein gegenteiliger Eindruck erweckt. Der Bundeswirtschaftsminister zog sogar den Schluss, nach den Stichproben und Anrufaktionen der Bundesagentur könne vermutet werden, dass die Arbeitslosigkeit um mindestens 10 Prozent überschätzt werde. Vor dem Hintergrund der Freiwilligkeit der Beantwortung der telefonisch gestellten Fragen ist die Herstellung eines Zusammenhangs zwischen der Nichtteilnahme an der Befragung und etwaigem Leistungsmissbrauch nicht hinnehmbar[44]. Die Datenschutzbeauftragten des Bundes und der Länder haben dazu eine

43 vgl. Anlagenband 2005, a. a. O.
44 Pressemitteilung „Datenschutz gilt auch für ALG II-Empfänger“ des Berliner Beauftragten für

Entschließung gefasst und festgestellt, dass die Ablehnung der Teilnahme an einer solchen Befragung nicht den Verdacht auf Leistungsmissbrauch rechtfertigt. Wer seine Datenschutzrechte in Anspruch nehme, dürfe deshalb nicht des Leistungsmissbrauchs bezichtigt werden. Gleichzeitig haben sie ihre rechtzeitige Beteiligung bei der bereits angekündigten erneuten Telefonaktion gefordert[45]. Ob derartige Telefonbefragungen überhaupt rechtlich zulässig sind, kann man mit Fug und Recht bezweifeln.

Die steigende Anzahl der an uns gerichteten Eingaben zeigt, dass die vielen offenen datenschutzrechtlichen Fragen im Zusammenhang mit der Einführung des Arbeitslosengeldes II den Bürgerinnen und Bürgern große Sorge bereiten. Im Folgenden haben wir einige der am häufigsten an uns herangetragenen Fragestellungen zusammengefasst:

Eine Vielzahl der uns telefonisch und schriftlich übermittelten Eingaben bezieht sich auf die Frage der datenschutzrechtlichen Zulässigkeit der Anforderung von Kontoauszügen. Betroffene sind verunsichert, wenn sie unter Hinweis auf ihre Mitwirkungspflicht nach dem Sozialgesetzbuch aufgefordert werden, die Kontoauszüge für häufig lange zurückliegende Zeiträume vorzulegen.

Eine pauschale Anforderung von Kontoauszügen lässt das Datenschutzrecht nicht zu. Dies gilt insbesondere dann, wenn den Betroffenen generell untersagt wird, einzelne Buchungen zu schwärzen. Wir haben gemeinsam mit den Landesbeauftragten für den Datenschutz der Länder Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein Hinweise zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen entwickelt[46]. Wir haben alle Jobcenter und Bezirksämter in Berlin aufgefordert, diese Hinweise zu beachten. Wir hoffen, dass den Betroffenen ein nützlicher Wegweiser an die Hand gegeben wird, und erwarten, dass die Sozialleistungsträger künftig mit Augenmaß nur die im Einzelfall erforderlichen Informationen erheben[47].

Häufig haben uns im Berichtszeitraum Beschwerden von Bürgerinnen und Bürgern erreicht, die sich über fehlenden Diskretionsschutz in den Jobcentern Berlins beklagten.

Datenschutz und Informationsfreiheit v. 21. Oktober 2005, abrufbar unter http://www.datenschutz-berlin.de/aktuelle/presse05/presse12.htm

45 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 27./28. Oktober 2005 "Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten", vgl. Anlagenband "Dokumente zu Datenschutz und Informationsfreiheit 2005", S. 17

46 die Hinweise sind abrufbar unter: http://www.datenschutz-berlin.de/doc/de/sonst/kontoauszuege.pdf

47 Pressemitteilung des Berliner Beauftragten für Datenschutz und Informationsfreiheit „Das Recht auf Schwärzung – Empfehlungen zur Vorlage von Kontoauszügen in Jobcentern und Sozialämtern“ v. 24. November 2005, abrufbar unter http://www.datenschutz-berlin.de/aktuelle/presse05/presse13.htm

Sie berichteten uns von überfüllten Wartezonen und Beratungsräumen, in denen es problemlos möglich war, Kenntnis von den persönlichen Verhältnissen des am Nebentisch ebenfalls zur Beratung sitzenden Hilfeempfängers zu nehmen.

In der Anfangszeit der Arbeitsaufnahme der Jobcenter war der fehlende Diskretionsschutz teilweise auf Umzugs- und Umbaumaßnahmen zurückzuführen, die durch die überstürzte Umsetzung der Hartz IV-Reform nötig wurden. Mittlerweile sollte diese Übergangszeit jedoch beendet sein. Nach den sozialdatenschutzrechtlichen Vorschriften sind die Jobcenter verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Vertraulichkeit zu gewährleisten. 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.

Verunsichert durch Presseberichte über geplante verstärkte Kontrollen von Leistungsbeziehern zur Bekämpfung des angeblichen Leistungsmissbrauchs durch erneute Telefonaktionen und Hausbesuche oder eigene Erfahrungen mit bereits durchgeführten Hausbesuchen wandten sich Bürgerinnen und Bürger an uns und baten uns um Auskunft, ob es zulässig ist, wenn von Mitarbeiterinnen und Mitarbeitern der Jobcenter Hausbesuche durchgeführt werden. Wir wurden gefragt, ob eine Verpflichtung besteht, diesen Eintritt in die Wohnung zu gewähren.

Die Durchführung eines Hausbesuches ist nicht von vornherein als datenschutzrechtlich unzulässig anzusehen. Allerdings sind an die Zulässigkeit strenge Anforderungen zu stellen. So dürfen Hausbesuche nur dann durchgeführt werden, wenn andere Möglichkeiten zur Aufklärung des Sachverhaltes nicht bestehen. Der Hausbesuch muss im konkreten Einzelfall erforderlich und verhältnismäßig sein. Die Mitarbeiterinnen und Mitarbeiter müssen sich durch Vorlage des Dienstausweises legitimieren. Der Betroffene muss zu Beginn auf den Grund des Hausbesuches hingewiesen werden. Auch sind die Mitarbeiterinnen und Mitarbeiter des Jobcenters nicht befugt, die Wohnung ohne Einwilligung des Betroffenen zu betreten. Allerdings ist dieser darauf hinzuweisen, dass eine Verweigerung des Zutritts ggf. Leistungskürzungen zur Folge haben kann.

Die Ablehnung eines unangekündigten Hausbesuchs rechtfertigt dagegen keine Leistungskürzung, denn in ihm ist nach der Rechtsprechung mehrerer Sozialgerichte ein Eingriff in das Grundrecht auf *Unverletzlichkeit der Wohnung* zu sehen. Auch bei der Durchführung von Haus-

besuchen ist ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren. Zwar ist ein Hausbesuch nicht mit einem Lauschangriff gleichzusetzen, in beiden Fällen wird der Mensch aber zum Objekt staatlicher Beobachtung in seiner Wohnung.

Das Bundesverfassungsgericht sieht in der Privatwohnung als „letztem Refugium“ ein Mittel zur Wahrung der *Menschenwürde*. Dies verlange zwar nicht einen absoluten Schutz der Räume der Privatwohnung, wohl aber absoluten Schutz des Verhaltens in diesen Räumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstellt. Dies ist auch bei Hausbesuchen zur Kontrolle des Empfangs von Sozialleistungen zu beachten.

Die vorstehenden Ausführungen verdeutlichen, dass bei der praktischen Umsetzung von Hartz IV noch eine Reihe datenschutzrechtlicher Fragen zu klären und teilweise gravierende Mängel zu beheben sind. Die Datenschutzbeauftragten des Bundes und der Länder haben im Frühjahr 2005 auf unseren Vorschlag eine Arbeitsgruppe eingerichtet, um die Umsetzung der Vorgaben des SGB II kontinuierlich datenschutzrechtlich zu begleiten. Wir hoffen, durch unsere Mitarbeit einen Beitrag leisten zu können, um im Interesse der in Berlin lebenden Betroffenen eine datenschutzgerechtere Verfahrensweise erreichen zu können.

3.3 „Rasterfahndung“ zur Bekämpfung der Geldwäsche

Nach § 14 Abs. 1 Nr. 1 Geldwäschegesetz (GwG) sind Kreditinstitute verpflichtet, Vorkehrungen dagegen zu treffen, dass sie zur Geldwäsche missbraucht werden können. § 14 Abs. 2 Nr. 2 GwG nennt als Vorkehrungen u. a. angemessene geschäfts- und kundenbezogene Sicherungssysteme und Kontrollen zur Verhinderung der Geldwäsche und der Finanzierung terroristischer Vereinigungen. § 25 a Kreditwesengesetz (KwG) verpflichtet die Banken zu einer ordnungsgemäßen Geschäftsorganisation. Nach § 25 a Abs. 1 Satz 3 Nr. 6 KwG umfasst diese auch angemessene, geschäfts- und kundenbezogene Sicherungssysteme gegen Geldwäsche und gegen betrügerische Handlungen zu Lasten des Instituts; bei Sachverhalten, die aufgrund des Erfahrungswissens über die Methoden der Geldwäsche zweifelhaft oder ungewöhnlich sind, hat das Kreditinstitut diesen vor dem Hintergrund der laufenden Geschäftsbeziehung und einzelnen Transaktionen nachzugehen.

Über die datenschutzrechtlichen Gefährdungen, die von *Research-Systemen* zur Bekämpfung der Geldwäsche ausgehen, hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit im Jahresbericht 2000[48] informiert. „Research“ ist die nicht auf den konkreten Anlass bezogene Recherche nach Anhaltspunkten, die auf Geldwäsche hindeuten. Die Recherche ist

48 JB 2000, 3.4

nicht auf eine bestimmte Person oder ein bestimmtes Konto gerichtet, sondern soll sich auf sämtliche Kontobewegungen sämtlicher Kunden beziehen. Die Implementierung von Research-Systemen stellt einen weitreichenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Bankkunden dar.

Research-Systeme suchen nach hinreichenden Anhaltspunkten für einen Geldwäsche-anfangsverdacht. Dem Wesen nach handelt es sich also um Ermittlungen im Vorfeld eines Verdachtes. Dieses der Rasterfahndung entsprechende Prinzip ist eine Umkehrung der üblichen Ermittlungstätigkeit. Es wird mit dem Ziel vorgegangen, Nichtverdächtige auszuschließen, bis sich aus diesem Kreis Verdächtige ergeben haben.

Der Gesetzgeber hat es versäumt, bereichsspezifische Rechtsgrundlagen zu schaffen, aus denen sich ergibt, in welchem Umfang Banken bei der Schaffung angemessener geschäfts- und kundenbezogener Sicherungssysteme personenbezogene Daten verarbeiten und nutzen dürfen. § 25 a Abs. 1 Satz 3 Nr. 6 KwG kommt als bereichsspezifische Regelung für flächendeckende Rasterungen nicht in Betracht. Diese Rechtsvorschrift ist zu unbestimmt, um als datenschutzrechtlicher Erlaubnistatbestand in Betracht zu kommen.

Die Aufsichtsbehörden können allerdings nicht die Augen davor verschließen, dass das Gesetz die Banken zur Schaffung angemessener geschäfts- und kundenbezogener Sicherungssysteme verpflichtet und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hierin in der Regel die Schaffung eines nicht anlassbezogenen Geldwäsche-Research-Systems sieht. Es war deshalb erforderlich, datenschutzrechtliche Anforderungen für Research-Systeme zur Aufdeckung von Geldwäsche zu erarbeiten und die Banken zu verpflichten, diese einzuhalten. Die folgenden Anforderungen ersetzen zwar nicht die vorzuziehende Schaffung bereichsspezifischer Regelungen, können aber dazu beitragen, die Gefährdung des informationellen Selbstbestimmungsrechts durch Geldwäsche-Research-Systeme zu reduzieren:

Geldwäsche-Research-Systeme der Banken sollen sich grundsätzlich auf anlassbezogene Rasterungen beschränken. Sofern die Gefährdungsanalyse und Risikogewichtung des einzelnen Geldinstituts eine größere Rasterungsdichte gebieten, da der nur anlassbezogene Ansatz zu keinem angemessenen geschäfts- und kundenbezogenen Sicherungssystem führt und keine ausreichende Kontrolle zur Verhinderung der Geldwäsche darstellt, ist eine flächendeckende Rasterung aller für eine Verdachtsakquirierung relevanten Kontobewegungen möglich. Dabei sind jedoch erhöhte Anforderungen an die Transparenz der Research-Systeme zu stellen und die schutzwürdigen Interessen der Betroffenen in besonderer Weise zu berücksichtigen. Der Einsatz der Research-Systeme zu anderen Zwecken als dem der Bekämpfung der Geldwäsche, Terrorismusfinanzierung und Betrug, z. B. zum Zwecke des

Marketing, ist ausgeschlossen.

Die Rechtsgrundlage für die Durchführung flächendeckender Rasterungen ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die Banken haben ein berechtigtes (Eigen-)Interesse daran, die gesetzlichen Vorgaben (§ 25 a Abs. 1 Satz 3 Nr. 6 KwG sowie § 14 Abs. 2 Nr. 2 GwG) zur Schaffung angemessener geschäfts- und kundenbezogener Sicherungssysteme zu erfüllen und zu verhindern, dass ihr Institut für Geldwäschezwecke missbraucht wird. Das berechtigte Interesse der Banken ist abzuwägen gegen die schutzwürdigen Interessen der Betroffenen am Ausschluss der Nutzung ihrer personenbezogenen Daten für Geldwäsche-Research-Systeme. Bei der Implementierung von Research-Systemen sind insbesondere noch § 3 a BDSG (Grundsatz der *Datenvermeidung* und *Datensparsamkeit*) und § 35 Abs. 2 Satz 2 Nr. 3 BDSG (Grundsatz frühestmöglicher Löschung) zu beachten.

Eine gemeinsame „Gefährdungsanalyse“, die nicht zwischen den verschiedenen Verdachtsfällen (Geldwäsche, Terrorismusfinanzierung, Betrug) unterscheidet, ist hinzunehmen, da die Banken bei der Mehrzahl der Parameter die Auffälligkeit nicht spezifizieren können. Der Grundsatz der Zweckbindung der Speicherung und unterschiedliche gesetzliche Anforderungen bei den einzelnen Verdachtsfällen erfordern allerdings eine Kennzeichnung bzw. Separierung der Datensätze, soweit und sobald dies möglich ist.

Die Bankkunden sind von der Bank über eine flächendeckende Rasterung aller Kontobewegungen zu informieren. Sofern sich diese Forderung nicht direkt aus § 4 Abs. 3 Satz 1 Nr. 2 BDSG ergibt, wird sie aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG hergeleitet. Den bei der Abwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG einzubeziehenden Interessen des Betroffenen ist durch ausreichende Transparenz Rechnung zu tragen. (Bei der Schaffung ausreichender Transparenz können die Banken von staatlicher Seite unterstützt werden, da mit Research-Maßnahmen zum Zwecke der Geldwäschebekämpfung gesetzliche Anforderungen umgesetzt werden, die vom Staat der Kreditwirtschaft zur Wahrung des Allgemeininteresses auferlegt worden sind.) Für die Mitteilung an den Kunden sind verschiedene Wege denkbar (Allgemeine Geschäftsbedingungen, Mitteilung in den Kontoauszügen oder im normalen Postverkehr, bei Neukunden Information bei Vertragsschluss).

Bei der Frage, wie alt der für das Research-System verwendete Datenbestand sein darf, ist das Erforderlichkeitsprinzip (§ 28 BDSG) und der Grundsatz frühestmöglicher Datenlöschung (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG) zu beachten. Der Datenbestand in Research-Systemen darf daher nicht älter sein, als dies nach den wissenschaftlichen statistischen Erkenntnissen und den Erfahrungen der Bankpraktiker zur Optimierung der Ergebnisse erforderlich ist. Die von den Banken erwähnte Speicherlänge von drei Monaten gibt insoweit einen ersten Anhaltspunkt.

Sollten statistische Erkenntnisse dazu führen, dass der Zeitraum von drei Monaten deutlich überschritten werden müsste, um zu besseren Ergebnissen zu gelangen, ist zu beachten, dass die Speicherung über einen zu langen Zeitraum auch trotz statistisch-wissenschaftlicher Rechtfertigung unverhältnismäßig und damit rechtswidrig sein kann, wie etwa die Speicherung über ein Jahr hinaus. Auffälligkeiten können demgegenüber auch längerfristig gespeichert bleiben, soweit es für eine längere Speicherung nachvollziehbare Gründe gibt. Für statistische Daten gibt es keine zeitliche Beschränkung.

Die Verwendung bestimmter Parameter muss sachlich nachvollziehbar sein. Dies gilt insbesondere bei „verdachtsfernen Parametern“. Bei der Begründung können bindende Äußerungen der Bankaufsicht und/oder der Strafverfolgungsbehörden (z. B. in sog. Typologiepapieren) berücksichtigt werden. Die Banken haben die von ihnen gewählten Kriterien einer Plausibilitätskontrolle zu unterziehen und das Ergebnis insbesondere bei verdachtsfernen Parametern schriftlich zu begründen. Auf Anforderung soll die Begründung der zuständigen Aufsichtsbehörde vorgelegt werden. Bei bestimmten, sensitiven Merkmalen, deren Nutzung diskriminierend sein kann, wie etwa dem Geschlecht oder der Nationalität, muss in der Begründung gesondert dazu Stellung genommen werden, warum die Festlegung des Parameters keine Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen darstellt.

Für die besonderen Arten personenbezogener Daten nach § 3 Abs. 9 gilt ein Scoring-Verbot. Diese Daten dürfen also nicht gerastert werden. Für sonstige sensitive Daten gilt grundsätzlich kein *Scoring-Verbot*, auch wenn diese Daten, wie etwa die Nationalität, Hinweise auf ein sensitives Datum (Rasse, Religion) geben können. Bei der Verwendung derartiger „sensitiver Parameter“ sind allerdings in besonderem Maße schutzwürdige Interessen des Betroffenen tangiert. Das bedeutet, dass die Benutzung „sensitiver Parameter“ nur dann gerechtfertigt sein kann, wenn sie eine besondere Aussagekraft für den Verdacht des Vorliegens von Geldwäsche, Betrug und Terrorismusfinanzierung haben. Ein Zusammenhang sollte, soweit möglich, statistisch nachgewiesen sein. Jedenfalls muss in der Begründung der von den Banken vorzunehmenden Plausibilitätskontrolle gesondert dazu Stellung genommen werden, warum die Rasterung nach einem derartigen Merkmal, z. B. nach einer bestimmten Nationalität, nicht überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt.

Soweit intelligente Research-Systeme dabei helfen, die Justierung und Gewichtung der Parameter vorzunehmen, bestehen hiergegen keine datenschutzrechtlichen Bedenken. Demgegenüber sind intelligente lernende Systeme, deren Arbeitsweise von den Banken als nach dem BDSG verantwortliche Stelle nicht mehr nachvollzogen werden kann, nicht durch § 28 BDSG gedeckt.

Die Rechtmäßigkeit eines Research-Systems orientiert sich auch an seinem Erfolg. Ein erfolgloses Research-System wäre unverhältnismäßig und damit rechtswidrig. Als Indiz für ein erfolgreiches Research-System kann die Zahl der Verdachtsanzeigen fungieren. Die Geldwäschebeauftragten müssen außerdem in der Lage sein, die cut-off-Fälle (vom Computer ermittelte Auffälligkeiten, die aufgrund der erreichten Punktzahl „von Hand“ überprüft werden müssen) zügig abzuarbeiten, damit verhindert wird, dass Kunden sich zu lange im Vorhof des Verdachts befinden. Die von den Banken genannte Zeitspanne von einem Monat ist insoweit zufriedenstellend.

Die anlassunabhängige Rasterung von Kontenbewegungen zur Bekämpfung der Geldwäsche führt zu weitreichenden Eingriffen in das informationelle Selbstbestimmungsrecht der Bankkunden und ist deshalb nur in engen Grenzen zulässig.

3.4 Immer wichtiger: Anonymisierung und Pseudonymisierung

Mit den Novellierungen des Bundesdatenschutzgesetzes und des Berliner Datenschutzgesetzes im Jahre 2001 kam die Verpflichtung neu in die Gesetze, dass schon bei der Vorbereitung (Planung, Gestaltung und Auswahl) des Einsatzes von informationstechnischen Verfahren das Ziel zu verfolgen ist, keine oder so wenig wie möglich personenbezogene Daten zu verarbeiten. Es ist von den Möglichkeiten der Anonymisierung und der Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Diese Verpflichtung ist kennzeichnend für eine neue Denkrichtung im Datenschutz: Der Datenschutz soll nicht nur durch die Abwehr von Beeinträchtigungen von Persönlichkeitsrechten durch den extensiven Einsatz von Informationstechnik erreicht werden, sondern auch durch eine datenschutzfreundliche Ausgestaltung dieses Einsatzes, die damit beginnt, in die Planungen einzubeziehen, von der Verwendung personenbezogener Daten abzusehen, wenn dies den Zielen des IT-Einsatzes nicht entgegensteht, und wenn doch, die Verwendung personenbezogener Daten auf das für die Ziele der Datenverarbeitung notwendige Maß zu beschränken.

Es ist nicht zu bestreiten, dass es in vielen IT-Verfahren in Wirtschaft und Verwaltung nicht ohne Personenbezug gehen kann, weil es gerade um die Belange einzelner Personen geht in ihrer Rolle als Bürger, als Empfänger von Leistungen, als wegen der Verstöße gegen Recht und Ordnung Verfolgte, aber auch als Kunden und Ansprechpartner. Dennoch ist es tägliches Geschäft der Datenschutzbeauftragten, Teile von Datensätzen auch in betont personenbezogenen IT-Verfahren in Frage zu stellen, die weniger aus Notwendigkeit als vielmehr aus subjektiven Nützlichkeitserwägungen („Nice to have“, „Man könnte sie vielleicht einmal brauchen...“) oder aus vermeintlich technischen Zwängen („Das gekaufte Standardverfahren sieht dies so vor ....“) verarbeitet werden.

Es geht jedoch nicht nur um die quantitative und qualitative Festlegung des Umfangs personenbezogener Daten in der Phase der Verfahrenseinführung. Es geht auch um die Dauer des Lebenszyklus personenbezogener Daten. Viele personenbezogene Daten, die unbestritten für die Abwicklung der Aufgaben in Verwaltung, Wissenschaft und Wirtschaft gebraucht wurden, werden irgendwann, spätestens dann, wenn sie für diese Aufgaben nicht mehr erforderlich sind, nicht mehr gebraucht. In vielen Fällen schließt sich dann eine Frist an, in der die Daten unter Beschränkung des Zugriffs und der Anwendungszwecke archiviert werden (Sperrung im Sinne

der Datenschutzgesetze), bevor sie gelöscht werden müssen.

Diese in der Vergangenheit gültige Beschreibung des Lebenszyklus personenbezogener Daten lässt außer Acht, dass Wirtschaft und Verwaltung häufig, die Wissenschaft fast immer, ein Interesse daran haben, die Daten für spätere Auswertungen vorzuhalten. Die Wirtschaft will ihre Kunden besser kennen lernen, um so besser auf die Bedürfnisse eingehen zu können (bzw. sie so besser und gezielter umwerben zu können) und sie besser an sich zu binden. Die moderne Verwaltung wünscht sich ebenfalls Kundenbindung, vor allem aber möchte sie ihre Verwaltungsprozesse und das dem zugrunde liegende politische Entscheidungsverhalten optimieren, um die Wirkung des Einsatzes begrenzter öffentlicher Mittel im Sinne ihrer Ziele zu optimieren (Controlling). Die empirischen Wissenschaften benötigen massenhaft Einzelangaben von Personen, um ihre wissenschaftlichen Thesen daraus abzuleiten.

In allen diesen Fällen, in denen es nicht mehr um die Identität der Personen geht, verlangen die o. g. Vorschriften, dass der Personenbezug aufzuheben ist, weil er eben nicht mehr erforderlich ist. Die Daten sind zu anonymisieren bzw. zu pseudonymisieren. In manchen Fällen wird dies sogar gesetzlich gefordert. Dazu vier Beispiele, die keineswegs Anspruch auf Vollständigkeit erheben.

- Artikel 6 Abs. 1 e) der Europäischen Datenschutzrichtlinie von 1995 verlangt von den Mitgliedstaaten, dass personenbezogene Daten nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiter verarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht.

- § 12 Landesstatistikgesetz verlangt, dass die personenbezogenen Hilfsmerkmale, die für die Prüfung der Schlüssigkeit und Vollständigkeit der Erhebungs- und Hilfsmerkmale (ggf. auch durch Nachfragen bei den Personen) notwendig sind, gelöscht werden, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. Sie sind zusätzlich von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren.

- § 27 Abs. 4 Landeskrankenhausgesetz und § 15 der Berufsordnung der Ärztekammer Berlin bestimmen, dass Patientendaten zum Zwecke der wissenschaftlichen Forschung nur offenbart werden dürfen, wenn der Patient ausdrücklich der personenbezogenen Offenbarung zugestimmt hat oder wenn die Anonymität des Patienten hinreichend gesichert ist.

- § 67 c Abs. 5 Satz 2 Sozialgesetzbuch X sieht vor, dass Sozialdaten, die für Zwecke der wissenschaftlichen Forschung und Planung erhoben oder gespeichert werden, zu anonymisieren sind, sobald dies nach dem Forschungs- oder Planungszweck möglich ist.

Anonymisieren ist nach § 4 Abs. 3 Nr. 7 BlnDSG „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“.

Diese Definition berücksichtigt die Beobachtung, dass das Weglassen von identifizierenden Merkmalen, die Rückschlüsse auf die Identität der Person zulassen, nur selten einen absoluten Schutz vor Reidentifizierung ermöglichen. Dies gilt um so mehr, je detaillierter die für Forschung, Planung oder Controlling verbleibenden anonymisierten Einzeldatensätze eine Person noch beschreiben. Dabei besteht ein Dilemma: Je präziser die angestrebten Ergebnisse von Forschung, Planung oder Controlling sein sollen, je detaillierter müssen die Ausgangsdaten sein, je höher ist aber auch das Risiko der zufälligen Reidentifizierung anhand der detaillierten Personenbeschreibung. Dabei folgt die zitierte Vorschrift dem Prinzip Hoffnung: Je größer der Aufwand ist, die Einzelangaben einer bestimmten oder bestimmbaren Person zuzuordnen, je geringer ist die Wahrscheinlichkeit, dass es zu einer zufälligen – aber aufwandsfreien – Reidentifizierung kommt.

Um der beschriebenen Gefahr zu begegnen, ist die Forderung nach *Datenvermeidung* und *Datensparsamkeit* auch so zu interpretieren, dass auch die Detailtreue der anonymisierten Ausgangsdaten daraufhin geprüft wird, ob sie für das angestrebte Ergebnis erforderlich ist: Ist das Geburtsdatum erforderlich oder reicht vielmehr die Altersangabe? Ist die Adresse erforderlich oder reicht vielmehr die Straße, der Block, der Ortsteil, der Bezirk, der Postleitzahlenbereich?

Bestehen die Methoden bei der Anonymisierung in dem Fortlassen Personen identifizierender Daten und möglicherweise anderer nicht weiter gebrauchter Angaben sowie in der Abstraktion verbleibender Daten, soweit dies dem Ziel nicht abträglich ist, so stellt die Pseudonymisierung erheblich höhere methodische Anforderungen.

Pseudonymisieren ist nach § 4 Abs. 3 Nr. 8 BlnDSG „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“.

Während die Anonymisierung die *Deanonymisierung* (Wiederherstellung des Personenbezugs) ein für alle Mal ausschließen soll, kommt es bei der Pseudonymisierung entweder darauf an, die Deanonymisierung in bestimmten wohl definierten Fällen einem bestimmten Personenkreis zu ermöglichen oder an den pseudonymisierten Daten nachträglich Änderungen oder Ergänzungen anzubringen, wenn dies im Lauf der Zeit geboten ist.

Im einfachsten Fall ist das im Gesetz genannte Kennzeichen eine laufende

Nummer, die dort vergeben und verwaltet wird, wo die Daten noch personenbezogen vorliegen müssen, z. B. als personenbezogene Daten in den papierenen oder elektronischen Patientenakten in einem Krankenhaus, das die pseudonymisierten Daten etwa zu Forschungszwecken oder zu epidemiologischen Gesundheitsaufgaben an Dritte herausgibt. Abgesehen von den Restrisiken durch zufällige Reidentifizierung, wie sie schon bei der Anonymisierung beschrieben wurden, können die Empfänger die Identität der Patienten nicht herausfinden, können aber ihre Ergebnisse mit dem Pseudonym an das Krankenhaus zurückgeben, wo sie der personenbezogenen Akte hinzugefügt werden und vielleicht zur Behandlung des Patienten beitragen können.

Komplexer und bei höheren Sicherheitsanforderungen angemessener sind Pseudonymisierungsverfahren mittels *Treuhänder*. Ein wichtiges Beispiel ist die Qualitätssicherung bei der Nierenersatztherapie QuasiNiere, über die schon gelegentlich berichtet wurde[49]. Die von den Behandlungseinrichtungen zu liefernden Meldungen enthalten die Identität der Patienten und der Behandlungseinrichtung sowie die für die Qualitätssicherung erforderlichen Behandlungsdaten. Sie werden bei einem Datentreuhänder, einem Notar, angeliefert. Dieser leitet die Behandlungsdaten an die Auswertestelle QuasiNiere weiter, ohne sie weiter zur Kenntnis zu nehmen, und pseudonymisiert die Identitätsmerkmale des Patienten und der Behandlungseinrichtung mit Hilfe einer eigens dazu entwickelten Software. Diese Software, die nur unter der Kontrolle einer Chipkarte des Datentreuhänders ablaufen kann, ordnet den Identitätsmerkmalen in einem mehrstufigen Verfahren einen willkürlich gewählten, dann aber fest bleibenden Tabellenwert zu, der dann mit einem symmetrischen Verschlüsselungsalgorithmus (Triple-DES) zum Pseudonym umgerechnet wird. Dieses Verfahren ist wegen der Symmetrie des Verschlüsselungsverfahrens nicht unumkehrbar. Die Rückführung des Pseudonyms auf die Identität ist aber nur über den Notar als Datentreuhänder möglich.

Ohne Treuhänder, aber mit getrennten Datenbanken für Patienten- und Behandlungsdaten und mit Zufallszahlen, wird die Pseudonymisierung für die Bereitstellung von Behandlungs- und Forschungsdaten in klinischen Forschungsnetzen im Rahmen der *Telematik-Plattform Medizinische Forschungsnetze* (TMF) konzipiert. Wird ein Patient erstmalig erfasst, so werden seine Identitätsdaten in einer Patientenliste verschlüsselt gespeichert. Gleichzeitig wird eine Zufallszahl ermittelt, die dem Datensatz als *Personenidentität* (PID) hinzugefügt wird. Diese PID wird an die Behandlungsdatenbank weitergereicht, in der ein abgesehen von der PID leerer Datensatz erzeugt wird. Wenn dann die Behandlungsdaten des Patienten eingetragen werden sollen, stellt der Rechner des behandelnden Arztes eine Anfrage an die Patientenliste, ob der Patient dort schon verzeichnet ist. Ist dies der Fall, so wird eine weitere Zufallszahl ermittelt und als *temporäre Identitität* (TempID) an den Arzt und an die Behandlungsdatenbank übermittelt.

49 zuletzt JB 2004, 4.4.2

Der Arzt meldet sich dann bei der Behandlungsdatenbank an, gibt die TempID an und kann damit die dort vorhandenen Daten abfragen, verändern oder ergänzen. Die TempID wird dann sofort gelöscht. Da die PID und die TempID in der Patientendatenbank nie und in der Behandlungsdatenbank nur kurzzeitig zusammengeführt werden, ist eine unzulässige Zusammenführung von Patienten identifizierenden Daten und Behandlungsdaten ausgeschlossen.

In die Behandlungsdatenbank wird bei Anlage des Datensatzes für einen Patienten eine weitere Zufallszahl eingetragen, die sog. *Laboridentität* (LabID). Diese LabID dient der Zusammenführung von wissenschaftlichen Laborproben mit den Behandlungsdaten ohne Kenntnis der Identität des Patienten. Da PID und LabID zusammen gespeichert werden, kann im Zusammenwirken von Systembetreuern und behandelndem Arzt und mit Genehmigung eines im Datenschutzkonzept vorgesehenen Ausschusses die Pseudonymität aufgehoben werden, um Laborergebnisse dem Patienten zugute kommen zu lassen.

Das Datenschutzkonzept der TMF findet u. a. Anwendung beim Austausch von medizinischen Bilddaten in der Pädiatrischen Onkologie und Hämatologie der Charité in Berlin.

In den zuletzt beschriebenen Beispielen ist die Kryptographie Teil des Pseudonymisierungskonzepts. In unterschiedlicher Form stellen in den beiden folgenden Beispielen kryptographische Verfahren selbst die Pseudonymisierungsmethode:

Im Zusammenhang mit dem automatisierten Verfahren „Personal und Statistik“ (PuSta) sind die Personaldaten nach § 9 Abs. 1 Nr. 1 Personalstrukturstatistikgesetz symmetrisch zu pseudonymisieren. Dabei werden durch Verschlüsselung von Namen, Vornamen und Geburtstag einerseits und der Personalnummer andererseits mit einem symmetrischen Verschlüsselungsverfahren (konkret Triple-DES) statistische Hilfsmerkmale erzeugt. Für die Klärung von Rückfragen der Statistikstelle, die aufgrund der Plausibilitätsprüfung entstehen können, werden die Hilfsmerkmale wieder entschlüsselt. Die unzulässige Depseudonymisierung ist unter Strafe gestellt.

Anders als bei der PuSta-Pseudonymisierung erfolgt bei dem Integrierten Fach- und Finanzcontrolling (IFFC) der sozialen Transferleistungen auf der Grundlage der Software ePBN[50] eine Einwegpseudonymisierung der Daten, bevor diese aus den personenbezogenen Fachverfahren in das Controlling-Verfahren der Senatsverwaltung für Finanzen eingespeichert werden. Diese Pseudonymisierung erfolgt mittels eines Hash-Algorithmus (in diesem Falle SHA-1), der aus bestimmten personenidentifizierenden und möglichst unveränderlichen Merkmalen

50 JB 2003, 3.4

Zeichenketten von 160 Bit Länge erzeugt. Sichere Hash-Algorithmen zeichnen sich dadurch aus, dass zum einen aus dem Ergebnis keine Rückrechnung auf die Ursprungsdaten möglich ist (*Einweg-Pseudonym*) und zum andern verschiedene Ausgangsmerkmal stets auch zu verschiedenen Zeichenketten führen (Kollisionsfreiheit).

Die Einwegverschlüsselung ist immer dann erste Wahl, wenn statistische oder wissen-schaftliche Untersuchungen durchgeführt werden, die die spätere Ergänzung oder Aktualisierung pseudonymisierter Datensätze notwendig machen, ohne dass der Datenempfänger die Möglichkeit haben darf, die Identität der Personen zu ermitteln. Neben dem Controlling mit sehr sensiblen personenbezogenen Sozialdaten für politische Entscheidungsprozesse ist die Einwegverschlüsselung auch für wissenschaftliche Forschungen im Bereich der Medizin geboten, bei denen bestimmte Patienten über einen längeren Zeitraum Gegenstand der Forschung sind.

Es gibt eindeutige Tendenzen dafür, dass die Nachnutzung personenbezogener Daten für Zwecke, bei denen der Personenbezug keine Rolle mehr spielt, für die Gewinnung von Daten für politische und wirtschaftliche Entscheidungsprozesse in Zukunft eine immer größere Rolle spielen wird. Umso wichtiger ist es für den Schutz der personenbezogenen Daten vor späterer Verwendung zu unbestimmten Zwecken, dass Anonymisierungs- und Pseudonymisierungs-methoden in solchen Projekten zur Selbstverständlichkeit werden.

3.5 Wie ist SPAM zu bekämpfen?

Unerwartete Nachrichten rufen beim Empfänger unterschiedliche Reaktionen hervor: Von Inhalt, Absender und Zeitpunkt einer Mitteilung hängt es ab, ob sie große Freude, Gleichgültigkeit, Trauer oder Ärger hervorruft. Dies gilt selbstverständlich auch, wenn die Nachricht als E-Mail über das Internet gesandt wird. Meist unerwünscht sind E-Mails, wenn sie in großer Zahl zu Werbezwecken oder mit betrügerischer Absicht versandt werden – und von Absendern, die ihre Identität nicht preisgeben.

Neue Technik – neue Möglichkeiten

Neben der Information über das World Wide Web (WWW) ist die Individualkommunikation per E-Mail der derzeit am häufigsten genutzte Dienst im Internet. Die Technik, die diesem Dienst zugrunde liegt, ist wie der Versand von Postkarten organisiert: Wie auf einer Postkarte kann der Absender nicht nur den Text, sondern auch seine Unterschrift bzw. Absenderadresse frei

wählen; die Nachricht wird ohne Umschlag bzw. unverschlüsselt versandt; jeder Postbote bzw. Server-Betreiber, der die Nachricht weiterleitet, kann die Nachricht unbemerkt lesen und verfälschen; und schließlich kann jeder, der den Briefkastenschlüssel bzw. das Kennwort des E-Mail-Kontos hat, die Nachricht abholen.

E-Mails erreichen ihren Empfänger allerdings in der Regel wesentlich schneller als Postkarten. Und sie sind billiger: Eine elektronische Nachricht kann mit sehr geringem zeitlichem Aufwand zu einem Bruchteil der Portokosten einer Postkarte versandt werden – selbst wenn sie an Millionen von Empfängern gerichtet ist.

Diese Eigenschaften tragen dazu bei, dass E-Mails die schriftliche Kommunikation zunehmend ersetzen: Dank *Internet-Café*, Digitalkamera und multimedialer E-Mail braucht niemand auf die farbige Illustration der Nachricht aus dem Urlaub zu verzichten; die „klassische“ Urlaubs-postkarte wird von E-Mails ersetzt, die ihr an Aussagekraft um nichts nachstehen. Dank „Attachments“ (Datei-Anhängen) kann man sogar die digitalisierten Unterlagen einer Stellen-bewerbung per E-Mail hinzufügen. Das Bewusstsein dafür, dass diese Praxis keinen ange-messenen Schutz der versandten Informationen bietet, scheint, obwohl kaum jemand seine Bewerbung auf einer Postkarte versenden würde, wenig verbreitet zu sein.

Die genannten Eigenschaften der E-Mail-Kommunikation prädestinieren diese Technik jedoch vor allem für eine Anwendung: Informationen, Ankündigungen und Werbung, die ein Absender möglichst weit verbreiten möchte, ohne dabei hohe Kosten in Kauf nehmen zu müssen, versendet er am besten auf elektronischem Wege. Den Absender kostet der Versand einer
E-Mail an Tausende oder Millionen Adressaten in etwa so viel bzw. wenig wie jeden einzelnen Adressaten der Abruf dieser Nachricht.

Sollten wir uns daher nicht freuen, dass eine moderne, für den Versender kostengünstige Methode zu werben oder uns zu informieren existiert, die noch dazu Papier und Druckaufwand spart und daher umweltfreundlich erscheint?

Neue Technik – neue Probleme

Abgesehen davon, dass die *E-Mail-Werbung* nicht zwangsläufig zu einem Rückgang anderer Werbeformen führt und die Umwelt vielleicht durch den zusätzlichen Energiebedarf beim Versenden und Empfangen vieler E-Mails stärker belastet wird, verlagert diese Technik die Probleme massenhaften Nachrichtenversands vor allem vom Versender zum Empfänger: Je mehr Versender von Informations- und Werbematerial die E-Mail-Adresse eines Empfängers

nutzen, desto mehr Kosten und Aufwand für den Abruf und das Aussortieren unerwünschter E-Mails hat der Empfänger zu tragen. Vor allem jedoch sieht die E-Mail-Technik keinen Schutz des Empfängers vor unerwünschter Werbung vor: Eine Technik, die dem „Bitte keine Werbung“-Aufkleber auf dem Hausbriefkasten entspricht, existiert derzeit nicht.

So haben sich unerwünscht zugesandte E-Mails (UBE: „Unsolicited Bulk E-Mail“ bzw. UCE: „Unsolicited Commercial E-Mail“ oder auch: „Junk Mail“) für deren Empfänger zu einer wahren Plage entwickelt. Der Begriff SPAM steht für "Spiced Ham And Meat" oder – schlimmer – „Specially Prepared Assorted Meat“: Ein seit 1937 hergestelltes Dosenfleisch, das bei den amerikanischen Soldaten im Zweiten Weltkrieg zur Standard-Verpflegung gehörte und angeblich bald dazu führte, dass der Begriff „SPAM“ allgemein für „Unerwünschtes“ benutzt wurde. Dass der Begriff für penetrant in großer Menge unerwünscht versandte E-Mails verwendet wird, ist wohl auf einen Sketch aus der 25. Folge von „Monty Python's Flying Circus“ von 1970 zurückzuführen, in dem ein Ehepaar zum Frühstück von der Bedienung ausschließlich Gerichte, die SPAM enthalten, angeboten bekommt, während ein Chor von Wikingern die Kommunikation zunehmend mit dem Gesang „SPAM! Lovely SPAM! Wonderful SPAM!“ übertönt.

Der Versender von SPAM wird im Allgemeinen als „Spammer“, wenn der Inhalt der E-Mail noch dazu betrügerische Zwecke verfolgt, gelegentlich als „Scammer“ bezeichnet.

Das Motiv für den Versand von SPAM liegt klar auf der Hand: Bei einigen Hundertausend bis zu Millionen versandter E-Mails bestellen mindestens ein paar Dutzend Adressaten überteuerte Ware oder fallen auf andere Tricks herein. Ein *Hacker-Angriff* auf einen einzigen Server, über den mit SPAM beworbene potenzsteigernde Mittel vertrieben wurden, brachte zu Tage, dass allein über diesen Server eine halbe Million Dollar umgesetzt wurde – bei einer Gewinnspanne von 90 Prozent des Umsatzes.

Zudem ist in den letzten Jahren eine Professionalisierung und ein Zusammenwachsen der Spammer- und der Virenprogrammierer-Szene zu beobachten: Spam wird verwendet, um Computerviren zu verbreiten, und die Computerviren enthalten zunehmend Funktionen, die den „infizierten“ Computer zum ferngesteuerten Versenden von SPAM nutzbar machen.

Rechtliche Regelungen für den E-Mail-Versand

Bis in die neunziger Jahre des vergangenen Jahrhunderts hinein genügten die Mechanismen der „Selbstregulierung“ des Internet: Die Konventionen der Netznutzung („Netiquette“) schrieben vor, dass Nachrichten nur gezielt,

sparsam und bei konkretem Bedarf versandt wurden. Als im März und April 1994 die amerikanischen Anwälte Laurence Canter and Martha Siegel für die Dienste ihrer Kanzlei warben, indem sie eine Informationen über die „Green Card“-Verlosung 1994 mehr als 5000 Mal verbreiteten (allerdings nicht per E-Mail, sondern über das „Newsnet“), ernteten sie noch einen Sturm der Entrüstung der Internet-Nutzer, so dass die Proteste den Server des Providers der Anwaltskanzlei blockierten und der Provider den Internet-Anschluss der Anwälte deaktivierte.

Inzwischen sind von mehr als 100 Milliarden E-Mails jährlich wahrscheinlich 60 bis 70 Prozent als SPAM einzustufen. Der bundesdeutsche Gesetzgeber hat dem Rechnung getragen, als er 2004 bei der Umsetzung der „Richtlinie für den Schutz persönlicher Daten und der Privatsphäre auf dem Feld der elektronischen Kommunikation“ (RL 2002/58/EG) des Europäischen Parlaments und des Rates im novellierten „Gesetz gegen den unlauteren Wettbewerb“ (UWG) in § 7 festschrieb, dass ein Fall unlauteren Wettbewerbs vorliegt, wenn ein „Marktteilnehmer in unzumutbarer Weise belästigt“ wird durch „Werbung, obwohl erkennbar ist, dass der Empfänger diese Werbung nicht wünscht“, „bei einer Werbung unter Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post, ohne dass eine Einwilligung der Adressaten vorliegt“ oder „bei einer Werbung mit Nachrichten, bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen“.

Allerdings bestehen Ausnahmen. Werbung „unter Verwendung elektronischer Post“ wird dann nicht als „unzumutbare Belästigung“ angesehen, wenn „1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, 2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, 3. der Kunde der Verwendung nicht widersprochen hat und 4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen“. Alle vier Kriterien müssen erfüllt sein, damit eine E-Mail-Werbung zulässig sein kann.

Die Gesetzgebung entspricht damit der ständigen Rechtsprechung des Bundesgerichtshofs (BGH), der bereits 1972 und 1985 in Urteilen zur Wettbewerbswidrigkeit der Fernschreib-werbung[51] und zur wettbewerbswidrigen Belästigung durch Werbung im Btx-Mitteilungsdienst - Btx-Werbung[52] die unverlangte Zusendung von Werbung mittels elektronischer Medien als

51 I ZR 54/71
52 I ZR 222/85

unzulässig angesehen hatte. Liegt keine Geschäftsbeziehung zwischen dem Werbendem und dem Empfänger der Werbung vor, wird darin in der Regel ein Eingriff in das Persönlichkeitsrecht des Empfängers bzw. (bei Firmen) ein Eingriff in einen eingerichteten und ausgeübten Gewerbebetrieb gesehen.

Der Gesetzgeber setzt der E-Mail-Werbung also vor allem wettbewerbsrechtliche Grenzen. Liegt also womöglich gar kein datenschutzrechtliches Problem vor?

SPAM und Datenschutz

Grundlage für den massenhaften Versand von E-Mails ist eine Sammlung von E-Mail-Adressen, die für diese Zwecke gesammelt werden. E-Mail-Adressen sind personenbezogene Daten, da der Bezug zu einer bestimmten Person entweder über die Adresse selbst oder in der Regel mit sehr geringem Aufwand durch Hinzuziehen zusätzlicher Informationen (etwa durch eine Recherche im Internet) hergestellt werden kann.

Da es – wie erwähnt – grundsätzlich durchaus zulässig ist, Werbung per E-Mail zu verbreiten, kommt es zur Beantwortung der Frage, ob der Versand von E-Mails zu Informations- oder Werbezwecken datenschutzrechtlich zulässig ist, vor allem darauf an, ob die E-Mail-Adressen rechtmäßig zum Zwecke des E-Mail-Versands erhoben und gespeichert wurden.

An dieser Stelle ist eine Unterscheidung wesentlich: Kommt die unerwünschte E-Mail aus einem Staat der Europäischen Union bzw. einem Land, das einen gleichwertigen Datenschutz bietet, oder kommt die E-Mail aus einem Land, in dem das Sammeln von E-Mail-Adressen und der Versand von E-Mail-Werbung keinen Verstoß gegen die geltende Rechtsordnung darstellt?

Im ersten Fall muss in der Regel eine Einwilligung des Empfängers in die Verwendung seiner E-Mail-Adresse zum Empfang von E-Mails zu Informations- oder Werbezwecken vorliegen, die geschäftsmäßig versandt werden, d. h. im Rahmen einer regelmäßig ausgeübten, nicht privaten Tätigkeit, unabhängig davon, ob ein kommerzielles Interesse vorliegt. Keine Einwilligung wird in den genannten Fällen des § 7 UWG benötigt. Der Versender der E-Mails muss im Zweifelsfall in der Lage sein, das Vorliegen einer Einwilligung des Empfängers nachzuweisen.

Im zweiten Fall kommt die unerwünschte E-Mail entweder nachweisbar aus einem Land, in dem die genannten datenschutzrechtlichen Voraussetzungen nicht gelten, oder von einem unbekannten Absender, dessen Aufenthaltsort zum Zeitpunkt des E-Mail-Versands ebenso wenig ermittelbar ist wie seine Identität. Ein Verstoß gegen datenschutzrechtliche Bestimmungen liegt

also wahrscheinlich nicht vor, und falls doch, ist er meist nicht verfolgbar, weil der Täter anonym bleibt. Und wie nicht anders zu erwarten, überwiegt dieser Fall zahlenmäßig bei weitem.

Weil dies so ist, empfehlen wir grundsätzlich, unerwünschte E-Mails zu ignorieren und sie ungelesen zu löschen. Diese Arbeit lässt sich durch Software zur *SPAM-Filterung* (beim E-Mail-Provider oder auf dem einzelnen Computer) bzw. durch den SPAM-Filter des E-Mail-Programms zum Teil automatisieren. Ein Software-basierter Schutz kann jedoch aus prinzipiellen Gründen die Unterscheidung, ob es sich bei einer E-Mail um eine erwartete oder um eine unerwünschte Nachricht handelt, nicht in jedem Fall korrekt vornehmen. Daher ist eine sporadische Sichtung der Absender und Betreffs aller als SPAM aussortierten E-Mails zu empfehlen. Wenn dabei der Eindruck entsteht, ein eindeutig identifizierbarer Absender verbreitet wiederholt unerwünschte Werbung per E-Mail, kann sich ein Vorgehen gegen die damit verbundenen datenschutzrechtlichen Verstöße lohnen.

Unsere Empfehlungen sowohl zum Versand von E-Mails an mehrere Empfänger als auch zum Umgang mit unerwünscht empfangenen E-Mails haben wir in einem Anhang zu diesem Bericht zusammengestellt.

3.6 Prüfung eines der größten Datenverarbeiter in Deutschland – der GEZ

Im September 2004 haben wir zusammen mit den Landesdatenschutzbeauftragten von Brandenburg, Bremen und Hessen eine mehrtägige Prüfung bei der von den öffentlich-rechtlichen Rundfunkanstalten beauftragten Gebühreneinzugszentrale (GEZ) in Köln durchgeführt. Ziel der Prüfung war es, sich angesichts einer steigenden Zahl von Bürgerbeschwerden einen Überblick über das bei der GEZ bestehende Datenschutz-niveau sowohl in rechtlicher als auch in technisch-organisatorischer Hinsicht zu verschaffen. Der gemeinsame Prüfbericht liegt den Intendanten der drei betroffenen Rundfunkanstalten zur Stellungnahme vor.

Die GEZ hat in erster Linie die Funktion eines Rechenzentrums, das die öffentlich-rechtlichen Landesrundfunkanstalten bei der gesamten Abwicklung des Einzugs der Rundfunkgebühren unterstützt. Sie verarbeitet dabei die Daten von bundesweit rund 40 Millionen Rundfunkteilnehmern. Aus datenschutzrechtlicher Sicht wird die GEZ für die Rundfunkanstalten im Rahmen einer Auftragsdatenverarbeitung als Auftragnehmerin tätig. Verantwortlich für die Datenverarbeitung bleibt somit die jeweilige Landesrundfunkanstalt als Auftraggeberin. In Berlin und Brandenburg ist dies der *Rundfunk Berlin-Brandenburg* (RBB). Der Berliner

Beauftragte für Datenschutz und Informationsfreiheit und die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg kontrollieren die Einhaltung des Datenschutzes daher nicht nur bei den wirtschaftlichen und administrativen Tätigkeiten des RBB, sondern auch bei der GEZ, soweit es sich um personenbezogene Daten von Bürgern Berlins und Brandenburgs handelt. Außerhalb von Berlin und Brandenburg ist eine entsprechende unabhängige Datenschutzkontrolle bisher nur bei Radio Bremen und beim Hessischen Rundfunk gegeben. In den übrigen ARD-Anstalten wird die Einhaltung des Datenschutzes ausschließlich durch interne Datenschutzbeauftragte der Rundfunkanstalten kontrolliert.

Bei der Prüfung konnte festgestellt werden, dass die GEZ dem Datenschutz grundsätzlich eine große Bedeutung beimisst. Insbesondere ist der Anspruch zu erkennen, ein hohes Maß an Datensicherheit zu gewährleisten. Die Sicherheitsvorgaben sind in entsprechenden Konzepten beschrieben. Es ist ein IT-Sicherheitsbeauftragter bestellt und die getroffenen technischen und organisatorischen Maßnahmen werden regelmäßig von der Innenrevision kontrolliert. Angesichts der Komplexität eines Großrechenzentrums wie der GEZ musste sich die Prüfung in dieser Hinsicht allerdings auf einige ausgewählte Bereiche beschränken. Dies war auch der Tatsache geschuldet, dass die GEZ im Prüfungszeitraum dabei war, ihr noch aus den 1970er Jahren stammendes Datenverarbeitungssystem durch ein neues System mit der Bezeichnung "DV 2005" zu ersetzen, das inzwischen in den Echtbetrieb übergegangen ist. Die Konzeption des neuen Systems sieht objektorientierte Programmiersprachen, relationale Datenbanken sowie die Trennung der Schichten vor und soll mehr Flexibilität gewährleisten.

Hinsichtlich des rechtlich zugelassenen Umfangs der Verarbeitung personenbezogener Daten durch die GEZ im Auftrag des RBB und der anderen Rundfunkanstalten hat sich gezeigt, dass es in vielen Fragen nach wie vor unterschiedliche Auffassungen bei den Landesdatenschutzbeauftragten auf der einen und den Rundfunkanstalten auf der anderen Seite gibt. Folgende Schwerpunkte haben sich bei der Prüfung ergeben:

Bearbeitung des Posteingangs

Bei der GEZ gehen täglich etwa 79.000 Briefe, Faxe und E-Mails ein. Die Bearbeitung des Posteingangs, d. h. das Öffnen der Briefe, das Scannen der Dokumente und die Entsorgung der Papierunterlagen durch ein privates Entsorgungsunternehmen, erfolgt datenschutzkonform. Werden Unterlagen durch externe Dritte als Datenverarbeitung im Auftrag vernichtet, ist die gesamte Handhabung und Sicherung der Unterlagen zwischen der

Übergabe und dem Abschluss der Vernichtung vertraglich festzulegen. Die GEZ hat einen entsprechenden Entsorgungsvertrag vorgelegt, der allerdings nicht ausdrücklich festschreibt, dass die Vernichtung der Akten entsprechend der Sicherheitsnorm DIN 32757 erfolgt. Die Ergänzung des Vertrags um eine solche Klausel wurde uns zugesagt.

Zugriffsrechte der GEZ-Sachbearbeiter

Die Sachbearbeitung bei der GEZ ist in der Weise organisiert, dass grundsätzlich keine Differenzierung nach örtlichen oder sachlichen Kriterien vorgenommen wird. Dies hat zur Folge, dass die Sachbearbeiter grundsätzlich bundesweit Zugriff auf alle Teilnehmerkonten haben.

Die Zugriffsberechtigungen und das darauf basierende Rollenkonzept bei der Verarbeitung personenbezogener Daten durch die GEZ sind aus datenschutzrechtlicher Sicht nicht zufrieden stellend, wurden aber als noch vereinbar mit den datenschutzrechtlichen Bestimmungen vorerst akzeptiert. Eine Beschränkung der Zugriffsrechte würde eine komplette Neuordnung der Organisationsstruktur der GEZ voraussetzen. Hier gilt es, gemeinsam mit den Rundfunk-anstalten und der GEZ an Lösungen zu arbeiten, die ein differenzierteres Zugriffskonzept ermöglichen, ohne dabei die Effizienzvorteile eines gemeinsamen Rechenzentrums aufzuheben.

Löschungskonzept *Teilnehmerhistorie*

Die sog. Teilnehmerhistorie protokolliert die Änderungen an den Stammdaten unter Verwendung von Funktionscodes (Protokolleinträge). In der Historie werden die Daten der Rundfunkteilnehmer aus dem laufenden und den vorangegangenen vier Jahren vollständig gespeichert. Zur Löschung von älteren Daten aus der Teilnehmerhistorie wird jährlich ein „Pflegelauf“ durchgeführt. Bei abgemeldeten Teilnehmerkonten werden dabei sämtliche Einträge gelöscht. Bei noch aktiven Konten bleiben die Stammdaten eines Teilnehmers erhalten.

Das zugrunde liegende Löschungskonzept der GEZ begegnet keinen datenschutzrechtlichen Bedenken. Die regelmäßige Speicherfrist von vier Jahren zuzüglich des laufenden Kalenderjahres ist gerechtfertigt. Die Datenverarbeitung innerhalb dieses Zeitraums ist für die Erfüllung der der GEZ zugewiesenen Aufgaben noch erforderlich. Bei der Prüfung sind an der praktischen Umsetzung dieses Konzepts allerdings Zweifel aufgetreten. Wir mussten feststellen, dass die Sachbearbeiter bei aktiven Teilnehmerkonten Zugriff auf frühere Wohnanschriften, frühere Kontoverbindungen oder vor langer Zeit gewährte Befreiungen von

der Gebührenpflicht einschließlich des Befreiungsgrundes haben.

Unabhängig von der Löschung der Daten aus der Teilnehmerhistorie speichert die GEZ die Historiedaten für weitere zwei Jahre auf Magnetbändern. Diese Archivierung ist datenschutzrechtlich akzeptabel. Die GEZ kann sich insoweit auf eine entsprechende Anwendung der handelsrechtlichen Aufbewahrungsfristen nach § 257 Handelsgesetzbuch berufen. Der Gebühreneinzug der GEZ ist Teil der Finanzbuchhaltung der Rundfunkanstalten, die ihrerseits nach handelsrechtlichen Grundsätzen bilanzieren.

Datenquellen und Briefaktionen der GEZ

Großer Raum wurde bei der Prüfung erneut der Verarbeitung personenbezogener Daten im Zusammenhang mit den sog. *Mailing-Aktionen* gewidmet, die die GEZ zur Ermittlung von sog. Schwarzsehern und -hörern einsetzt. Die Briefaktionen, mit denen die Empfänger der Schreiben zur Anmeldung von Rundfunk- und Fernsehgeräten bewegt werden sollen, werden seit 1981 durchgeführt. Der Kreis der Adressaten wurde in dieser Zeit kontinuierlich erweitert. Wurden zu Beginn lediglich Personen, die nur als Hörfunkteilnehmer bei der GEZ gemeldet waren, angeschrieben, zählen mittlerweile auch abgemeldete Teilnehmer, Jugendliche, private Haushalte sowie Unternehmen und Selbstständige zu den Zielgruppen. Die Adressen für die Mailing-Aktionen erhält die GEZ zum einen im Rahmen regelmäßiger Übermittlungen von den Einwohnermeldeämtern und zum anderen durch Anmietung bei kommerziellen Adresshändlern. Im Jahr 2003 verschickte die GEZ ca. 18,7 Millionen Schreiben (10,4 Millionen Erstbriefe und 8,3 Millionen Erinnerungsbriefe).

Der GEZ werden im Falle eines Umzugs (Anmeldung und Abmeldung) oder beim Tod eines Einwohners von den Meldebehörden automatisch bestimmte Daten – unter anderem Namen und Vornamen, neue und alte Anschrift sowie Geburtsdatum – übermittelt. Wesentliche datenschutzrechtliche Bedenken bestehen insoweit nicht. Die monatliche Meldedaten-übermittlung stützt sich auf entsprechende Rechtsverordnungen in den Ländern, deren Erlass die Datenschutzbeauftragten allerdings kritisiert hatten[53]. Der von der GEZ vorgenommene Abgleich der gelieferten Daten mit dem Gesamtbestand der GEZ sowie die daran an-knüpfenden Briefaktionen halten sich im Rahmen des vorgegebenen Übermittlungszwecks. Auch die Aktualisierung der Anschriften im Datenbestand der GEZ ist mit dem in den Übermittlungsverordnungen vorgesehenen Verwendungszweck noch vereinbar.

Anders beurteilt sich hingegen der Erwerb von Adressdaten beim privaten Adresshandel. Hierbei geht es in erster Linie um Daten solcher Personen, bei denen die GEZ einen besonders hohen Anteil an Schwarzsehern und -hörern vermutet, wie z. B. Abonnenten von Fernsehzeitschriften oder des PayTV, Teilnehmer an Gewinnspielen von Rundfunksendern oder Kunden bestimmter E-Mail-Anbieter. Insgesamt bezieht die GEZ auf diesem Weg pro Jahr rund 85 Millionen Adressdatensätze. Diese Praxis ist nach dem geltenden Recht, trotz einer zum 1. April 2005 erfolgten Änderung des Rundfunkgebührenstaatsvertrages, nach wie vor unzulässig. Darauf haben wir bereits in unserem letzten Jahresbericht hingewiesen[54]. Der Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und Ländern hat - unterstützt durch einige Datenschutzbeauftragte der Rundfunkanstalten - den Rundfunkreferenten Vorschläge zur

53 JB 1996, 4.2.1
54 JB 2004, 5.3

Änderung des Rundfunkgebührenstaatsvertrages unterbreitet, die für mehr Rechtsklarheit sorgen sollen. Der Regelungsentwurf sieht vor, dass die Erhebung der Daten und auch ihre weitere Verwendung ausschließlich zu dem Zweck der Feststellung, ob ein Teilnehmerverhältnis vorliegt, zulässig sind. Die Befugnis ist zudem auf solche Daten beschränkt, die überhaupt geeignet ist. Rückschlüsse auf eine mögliche Gebührenpflicht zu ziehen. Jede Rückübermittlung von Daten an die Absender ist ausdrücklich untersagt. Dies ist zwar schon nach geltendem Recht wegen des Grundsatzes der Zweckbindung nicht zulässig. Gleichwohl ist es ständige Praxis der GEZ, nicht-zustellbare Anschriften zur Geltendmachung von Gewährleistungsansprüchen an die Adresshändler zurückzumelden. Schließlich wird ein Widerspruchsrecht vorgeschlagen, das es den Betroffenen ermöglichen soll, jede weitere Verwendung der vom Adresshandel gelieferten Daten zu unterbinden.

Musterschreiben

Angesichts häufiger Beschwerden über den Inhalt der von der GEZ versandten Formschreiben, aber auch über den teilweise darin angeschlagenen wenig freundlichen Ton haben wir sämtliche Muster dieser Schreiben aus datenschutzrechtlicher Sicht geprüft. Wir haben dabei festgestellt, dass in zahlreichen dieser Schreiben den Empfängern unter Androhung von Maßnahmen des Verwaltungszwangs eine Pflicht zur Beantwortung der Schreiben auch dann suggeriert wird, wenn eine solche Pflicht nicht besteht. Hier haben wir dem RBB entsprechende Änderungen empfohlen.

Zugriff auf Teilnehmerkonten anderer Landesrundfunkanstalten

Die Datenbestände der GEZ werden in einem einzigen bundesweiten Bestand mit einem eindeutigen Ordnungsbegriff, der neunstelligen Teilnehmernummer, gespeichert und sind nur logisch nach der Zugehörigkeit zu den verschiedenen Landesrundfunkanstalten getrennt. Die Gebührenabteilungen der Landesrundfunkanstalten haben einen wechselseitigen Online-Zugriff auf sämtliche Teilnehmerkonten. Dieses Verfahren ist aus Sicht des Datenschutzes nur akzeptabel, wenn durch technische und organisatorische Maßnahmen sichergestellt ist, dass Abrufe nur im begründeten Einzelfall erfolgen. Deswegen verpflichtet der RGebStV die übermittelnde Landesrundfunkanstalt zur Protokollierung der Datenzugriffe. Die bei dem Abrufverfahren praktizierte Protokollierung weist jedoch Mängel auf. Wir haben insbesondere eine Präzisierung der Abfragegründe gefordert.

Online-Zugriff der *Gebührenbeauftragten* auf den Datenbestand der GEZ

Datenschutzrechtlich bedenklich ist auch der Umfang, in dem die als Außendienstmitarbeiter tätigen Rundfunkgebührenbeauftragten auf den Datenbestand der GEZ zugreifen können. Auch diese haben seit einiger Zeit einen bundesweiten Online-Zugriff auf alle Teilnehmerkonten, obwohl sich ihre Zuständigkeit nur auf bestimmte Gebiete innerhalb des Sendegebiets einer einzigen Rundfunkanstalt beschränkt. Die Erforderlichkeit des bundesweiten Zugriffs konnte von der GEZ bisher nicht überzeugend begründet werden.

Beauftragung privater Dritter mit der Datenverarbeitung

Die GEZ führt angesichts des Umfangs der im Zusammenhang mit der Erhebung der Rundfunkgebühren zu verarbeitenden Daten nicht alle Datenverarbeitungsleistungen selbst durch. Vielmehr werden einige Aufgaben an externe private Dienstleister vergeben (z. B. Datenerfassung, Betrieb von Call-Centern, Druck und Versand von Post). Dies ist im Rahmen einer Datenverarbeitung im Auftrag zulässig. Die Beauftragung bedarf allerdings einer schriftlichen Vereinbarung. Was die inhaltliche Ausgestaltung dieser Verträge angeht, besteht Nachbesserungsbedarf.

Bei der Prüfung der Datenverarbeitung der GEZ wurde eine Reihe von Mängeln festgestellt, für deren Behebung wir Vorschläge gemacht haben. Die anstehende Modernisierung der Datenverarbeitungstechnik bietet die Chance, diese zügig umzusetzen. Wir werden den Prozess konstruktiv begleiten. Der außergewöhnliche Umfang der bundesweiten Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einzug der Rundfunkgebühren erfordert zudem eine regelmäßige Prüfung der Einhaltung des Datenschutzes in diesem Bereich.

4. Aus den Arbeitsgebieten

4.1 Öffentliche Sicherheit

4.1.1 Polizei

DNA-Analysedatei

Das Bundeskriminalamt hatte auf Wunsch der Datenschutzbeauftragten des Bundes und der Länder eine Auswertung der DNA-Analysedatei vorgenommen, die ein datenschutz-rechtliches Problem deutlich werden ließ.

Mit Stand vom 11. Oktober 2004 enthielt die Datei – aufgeschlüsselt für die einzelnen Bundesländer – folgende Zahl von Datensätzen:

Bundesland	Anzahl
Baden-Württemberg	65.641
Bayern	70.771
Berlin	10.516
Brandenburg	8.509
Bremen	1.878
Hamburg	9.453
Hessen	31.167
Mecklenburg-Vorpommern	5.542
Niedersachsen	34.419
Nordrhein-Westfalen	58.428
Rheinland-Pfalz	20.521
Saarland	4.030
Sachsen	27.139
Sachsen-Anhalt	9.920
Schleswig-Holstein	7.486
Thüringen	6.762

In Berlin entfallen die Speicherungen im Wesentlichen auf folgende Delikte:

Delikt	Anzahl
Straftat gegen Leben	1.217
Sexualdelikte	1.870
Diebstahlsdelikte	3.527
Raub/Erpressung	2.664
Körperverletzung	526
Gemeingefährliche Straftaten	390

Aber auch bei Betrug/Untreue (5 Fälle), Sachbeschädigung (6), Straftaten gegen die öffentliche Ordnung (11), Widerstand gegen die Staatsgewalt (2), Straftaten in Bezug auf Religion/Weltanschauung (3) und Straftaten im Amt (1 Fall) wurden Daten aus Berlin eingestellt. Andere Länder speisten die DNA-Analyse-Datei bei dem BKA in Fällen von falscher uneidlicher Aussage und Meineid, Straftaten gegen Personenstand, Ehe und Familie, strafbarem Eigennutz, Verstößen gegen das Ausländergesetz, das Asylverfahrensgesetz und das Arzneimittelgesetz, falscher Verdächtigung und Geld- und Wertzeichenfälschung.

Diese Delikte sind jedoch nicht in dem Katalog der Anlage zu § 2 c DNA-Identitätsfeststellungsgesetz (DNA-IFG) enthalten und ohne zusätzliche Informationen nicht als Straftat von erheblicher Bedeutung zu erkennen (§ 31 g StPO). Der Polizeipräsident hat uns dazu mitgeteilt, dass der Gesetzgeber bewusst darauf verzichtet hat, einen abschließenden Katalog als Speicherungsvoraussetzung anzugeben. Sinn und Zweck einer solchen Verfahrensweise ist es, eine möglichst flexible und an die Lage angepasste Handhabung, vor allem aber auch Bestückung der Datei zu gewährleisten. Gleichwohl muss der unbestimmte Rechtsbegriff der Straftat von erheblicher Bedeutung durch Auslegung konkretisiert werden. Dabei sind verfassungsmäßige Vorgaben, insbesondere der Grundsatz der Verhältnismäßigkeit, zu berücksichtigen. Der Polizeipräsident hat sich dabei an dem polizeirechtlichen Begriff orientiert (§ 17 Abs. 3 ASOG). Im aktuellen Datenbestand nennt der vermerkte Erfassungsgrund nicht in allen Fällen die Straftat, die die Datenspeicherung rechtlich begründet hat. So kommt es bereits bei der Sicherung von Spuren am Tatort zur Festlegung der Spurennummern/ISVB- bzw. POLIKS-Vorgangsnummern. Wird die anlässlich einer minderschweren Straftat gesicherte DNA-Spur mit einer erheblichen Straftat (in der keine *DNA-Spur* gesichert wurde) in einem Sammelvorgang verbunden, liegen die rechtlichen Voraussetzungen für eine Datenspeicherung vor.

Um die bestehende Spurenzuordnung und die sich daraus ergebende Beweiskette im Gesamt-ermittlungsverfahren nicht zu gefährden, wird die Spur in der DNA-Analysedatei jedoch unter der ursprünglichen Spurennummer und dem Ursprungsdelikt erfasst, auch wenn dieses inzwischen als Teil eines Sammelvorgangs oder einer Tatserie zu einem

erheblichen Delikt ge-worden ist. Die Eingabe mehrerer Erfassungsgründe zu einem Datensatz ist in der Datei nicht möglich. Weiterhin ist es eine übliche Vorgehensweise, den Beschluss nach § 2 DNA-Identitäts-feststellungsgesetz im Zuge einer aktuellen Verurteilung zu erlassen, die nicht zwangsläufig aufgrund einer Katalogstraftat erfolgt, dann aber im Beschluss auf die vorangegangenen Verur-teilungen wegen Katalogstraftaten zu verweisen. Auch in diesen Fällen ist der Erfassungsgrund in der Datei nicht mit der Straftat/Verurteilung identisch, aufgrund derer die retrograde Er-fassung veranlasst wurde. Diese ermittlungs- und verfahrenstechnischen Abläufe führen dazu, dass als Erfassungsgrund in der DNA-Analysedatei auch Straftaten gespeichert sind, die nicht von erheblicher Bedeutung oder nicht im Katalog der Anlage zu § 2 c DNA-IFG enthalten sind.

Dazu haben wir Folgendes festgestellt:

Nach der Errichtungsanordnung darf der Tatvorwurf (Angabe der gesetzlichen Vorschriften und nähere Bezeichnung der Straftaten) gespeichert werden. In Verbindung mit der Zweckbe-stimmung der DNA-Analysedatei kann es sich dabei nur um den die DNA-Analyse be-gründenden und rechtfertigenden Tatvorwurf handeln. Somit handelt es sich immer dann, wenn nicht der Tatvorwurf gespeichert ist, der die Speicherung auch rechtfertigt, um unrichtige Daten, die nach § 32 Abs. 1 BKAG zu berichtigen sind. Das Problem mit der Spurenzuordnung und Gefährdung der Beweiskette ist technisch-organisatorisch und nicht mit der Speicherung unrichtiger Daten zu lösen. Im Ergebnis wurde der Erfassungsgrund für alle in die Stichproben-untersuchung einbezogenen DNA-Spuren berichtigt. Zu weiteren Verfahren wurden die zuständigen Ermittlungsdienststellen gebeten, die zugrunde liegende Straftat von erheblicher Bedeutung festzustellen, um entsprechende Korrekturen, anderenfalls die Löschung des betroffenen Datensatzes zu veranlassen. Zu anderen Verfahren sollen die die Erheblichkeit begründenden Umstände festgestellt werden.

In der DNA-Analysedatei dürfen nur die Tatvorwürfe gespeichert werden, die die Speicherung begründen und rechtfertigen.

POLIKS

Im vergangenen Frühjahr ist das neue *Polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung* (POLIKS) in Betrieb gegangen. Damit wurde das alte Informationssystem Verbrechensbekämpfung (ISVB) abgelöst. Gleich zu Beginn hatte der Polizeipräsident in Berlin mit technischen Schwierigkeiten zu kämpfen. So häuften sich die Beschwerden darüber, dass sich Anzeigen und Anfragen nur mit Verzögerungen bearbeiten ließen. Zwischenzeitlich sollen Presseberichten zufolge keine Melderegisteranfragen möglich gewesen sein. Der Polizeipräsident in Berlin hat erklärt, dass bei der Einführung eines so komplexen Systems wie POLIKS fachliche und technische Schnittstellen unterschiedlichster Art aufeinander abgestimmt werden müssten. Weiterhin sei es verständlich, dass es nach Beginn des Echt-Betriebes noch Bedarf gebe, das System weiterzuentwickeln, um die Anforderungen der Fachdienststellen besser berücksichtigen zu können. Die Beseitigung der aufgetretenen Fehler wird noch einige Zeit in Anspruch nehmen. Der Polizeipräsident in Berlin rechnet dabei mit einem Zeitraum von etwa eineinhalb Jahren, bis allen Anforderungen der Fachdienststellen entsprochen sein wird. Im Übrigen habe die Polizei alle Melderegisterauskünfte über Personen bekommen. Lediglich spezielle Suchabfragen (z. B. die Namen aller Bewohner eines Hauses) waren zeitweise nur erschwert möglich.

POLIKS besteht aus drei Dateien: dem Vorgangsbearbeitungs-, dem Informationssystem und der elektronischen kriminalpolizeilichen Personenakte. Mit dem Vorgangsbearbeitungssystem erfolgt die geschäftsmäßige Bearbeitung eines polizeilich relevanten Ereignisses von der Erkenntnis-erlangung über die Vervollständigung und Verifikation bis hin zur Dokumentation. Dabei sind die besonderen Umstände, die Vorgeschichte und die Folgen bis zur Abgabe an eine außerpolizeiliche Stelle oder zur Archivierung zu dokumentieren. Das Informationssystem dient den Dienstkräften im Bereich des Vollzugsdienstes der Berliner Polizei zur Information. Mit seiner Hilfe sollen Schnell-auskünfte zu Personen, Sachen, Institutionen und Vorgängen durch gezielte Anfragen bzw. Recherchen ermöglicht werden. Das System soll den Beamten in ihrer eigenen Aufgabenwahr-nehmung ebenso dienen wie schnelle und zuverlässige Auskünfte zum Vorteil des Bürgers ermöglichen, um dessen Interessen schnellstmöglich wahrnehmen bzw. bei Beeinträchtigungen auf ein Mindestmaß beschränken zu können. Die elektronische kriminalpolizeiliche Personenakte ist eine Dokumentensammlung zur sachgerechten Wahrnehmung polizeilicher Aufgaben auf den Gebieten der Verfolgung von Straftaten sowie der vorbeugenden Verbrechensbekämpfung und Gefahrenabwehr. Dabei soll sie insbesondere das Erkennen von Tatzusammenhängen und die Aufklärung von Sachverhalten, die Feststellung von Tatverdächtigen und die Unterstützung der Personenidentifizierung und die Erlangung von Hinweisen für das polizeitaktische Vorgehen sowie die Eigensicherung ermöglichen.

Für jede automatisierte Datei über personenbezogene Daten ist eine *Errichtungsanordnung* zu erlassen (§ 49 ASOG). Die Errichtungsanordnung soll die *Transparenz* der Datenverarbeitung

gewährleisten (§ 5 Abs. 2 Nr. 5 BlnDSG). Die Errichtungsanordnung hat somit die Verarbeitung personenbezogener Daten in nachvollziehbarer Weise so darzustellen, dass die zur Aufgabenerfüllung erhobenen und gespeicherten Daten aufgabenbezogen dargestellt und die Befugnisse zur Verarbeitung im Hinblick auf die verfolgten Verarbeitungszwecke nachvollziehbar und abschließend beschrieben werden.

Diesen Anforderungen genügten die uns vorgelegten Entwürfe von Errichtungsanordnungen für die in POLIKS enthaltenen Dateien nicht hinreichend. Selbst unter Berücksichtigung, dass POLIKS den Anspruch erhebt, das gesamte Spektrum der Arbeit der Vollzugspolizei abzubilden, müssen die allgemeinen Anforderungen an eine Errichtungsanordnung erfüllt sein, damit die Datenverarbeitung auch überprüft werden kann. Zwar haben sich die Auffassungen zwischen uns und der Senatsverwaltung für Inneres mittlerweile angenähert; dennoch sind wir im Berichtszeitraum noch nicht zu einem abschließenden Ergebnis gelangt. Der Anspruch, das gesamte Spektrum polizeilichen Handelns abzubilden, kollidiert mit dem funktionalen Behördenbegriff (§ 4 Abs. 3 Nr. 1 BlnDSG). Danach ist Daten verarbeitende Stelle jede Behörde oder sonstige öffentliche Stelle, die die Daten für sich selbst verarbeitet oder verarbeiten lässt; nimmt eine öffentliche Stelle unterschiedliche gesetzliche Aufgaben wahr, so gilt diejenige Organisationseinheit als Daten verarbeitende Stelle, der die Aufgabe zugewiesen ist.

Das POLIKS-System ist sehr flexibel und enthält viele Möglichkeiten. Der Sinn und Zweck der Errichtungsanordnung besteht gerade darin, Festlegungen zu treffen, um eine Überprüfung der Datenverarbeitung zu ermöglichen, ohne dass dadurch die Flexibilität des Verfahrens leidet. Das wird vom Polizeipräsidenten und der Senatsverwaltung für Inneres im Kern genauso gesehen. Anderenfalls wäre das bereits vorgelegte umfangreiche Rollenkonzept entbehrlich.

Einvernehmen mit der Senatsverwaltung für Inneres bestand darüber, dass in den Errichtungsanordnungen die Prüffristen für Datenspeicherungen zur Aufgabenerfüllung und zur Vorgangsverwaltung bzw. befristeten Dokumentation voneinander abzugrenzen sind. Daten, die nur zu Dokumentations- bzw. reinen Verwaltungszwecken gespeichert werden, müssen dem Zugriff für die sonstige Aufgabenerfüllung entzogen werden. Das ist in den Errichtungsanordnungen klarzustellen.

Gerade die Einführung eines so komplexen und mächtigen Verfahrens wie POLIKS erfordert besondere Vorkehrungen zur Sicherstellung der Transparenz und Kontrollierbarkeit polizeilicher Datenverarbeitung.

Rosa Listen

Im Sommer wurde in der Presse darüber berichtet, dass die Polizeibehörden der Bundesländer Bayern, Thüringen und Nordrhein-Westfalen immer noch in ihren Polizeisystemen die Registrierungsmöglichkeiten für Homosexuelle als Tätergruppe und ihre Aufenthaltsorte als mögliche Tatorte enthalten.

Wir haben daraufhin geprüft, wie das Verfahren in Berlin aussieht. Nach mehreren Gesprächen hat uns der Polizeipräsident in Berlin mitgeteilt, dass Hinweise auf die sexuelle Orientierung von Personen den Datenbeständen der Berliner Polizei allenfalls in *POLIKS*, dem landesweiten Polizeilichen Informations- und Kommunikationssystem, zu entnehmen sind. Das kann als Katalogbegriff oder freitextlich – d. h. mit individueller Eingabe – geschehen. Als Katalogbegriff gibt es folgende Möglichkeiten:

Bezug	**Katalogbegriff**
Tatörtlichkeit	Homo-Treffpunkt Strichgebiet Strichplatz
Opfertyp	Homosexueller Strichjunge Stricher
Opferkreis	Homosexueller Strichjunge Stricher
Täterkreis	Homosexueller Strichjunge Stricher
Vorgehensweise des Täters	Angeblicher Homosexueller

Der Freitext ist vollständig variabel. Beide Eingabeformen sind nicht personen-, sondern fallbezogen ausgerichtet, so dass sie auch nur dementsprechend recherchierbar sind. Das bedeutet, dass im Fall einer personenbezogenen Überprüfung keinerlei Hinweis auf die sexuelle Orientierung ersichtlich wird. Das wird erst möglich, wenn über die Personenabfrage hinaus gezielte Daten zu gespeicherten Vorgangsnummern (Anwendungsfällen) im Wege der Sachbearbeitung abgefragt werden. Die Vorgangsnummern lassen sich auch dadurch ermitteln, dass der jeweilige Katalogbegriff eingegeben wird. In diesem Fall werden allerdings die Vorgangsnummern ohne spezielle Personenzuordnung ausschließlich nach dem Katalogbegriff ausgeworfen. Gezielt suchfähig sind diese Informationen also dann nicht, wenn auf diesem Wege eine bestimmte Person recherchiert werden soll; eine solche theoretische Möglichkeit hätte keine praktische Relevanz. Gleiches gilt für die Suche eines Begriffes über den Freitext. Zwar ist eine solche Recherche theoretisch ebenfalls möglich; das System würde aber sämtliche in ihm gespeicherten Vorgänge entsprechend abfragen, was regelmäßig zu einer

Überlastung und damit zu einer Systemabschaltung führen würde. Auch diese Möglichkeit ist folglich praktisch nicht relevant. Sinn und Zweck dieser vorgangsausgerichteten Recherchemöglichkeit ist das Erstellen von Lagebildern und das Erkennen von Brennpunkten. Entsprechend dieser eingeschränkten Verwendbarkeit sind aktuell in POLIKS elf Tatörtlichkeiten unter den Katalogbegriffen „Strichgebiet“ bzw.“ Homo-Treffpunkt“ registriert. Hinzu kommen – bedingt durch den Datenimport aus dem früheren System ISVB – weitere elf Tatörtlichkeiten unter dem Katalogbegriff „Strichgebiet“. Daneben sind seit dem Start von POLIKS drei Opfer von Straftaten als Zusatz zur Eingabe im konkreten Anwendungsfall mit dem Katalogbegriff „Homosexueller“ gespeichert worden.

Im Zuge unserer Aktivitäten und der damit verbundenen Sensibilisierung bei der Polizei wurde geprüft, inwieweit die bisher verwendeten Katalogbegriffe im Zusammenhang mit Straftaten an Homosexuellen und durch Homosexuelle noch eine kriminalistische und präventiv-polizeiliche Bedeutung entfalten. Das Landeskriminalamt Berlin hält die bisher verwendeten taktischen Begriffe (Katalogbegriffe der Tabelle, s.o.) inzwischen für entbehrlich. Grund dafür sind die seltene Verwendung bei der Eingabe eines Anwendungsfalles und die sehr geringe Bedeutung bei der Ermittlungsarbeit. Eine Ausnahme bildet der als Rollenvorspiegelung zum modus operandi vorgesehene Katalogbegriff „Angeblicher Homosexueller“; dieser soll auch künftig verwendet werden. Hierbei ist kennzeichnend, dass sich der Täter nur als Homosexueller ausgibt, um mit seinem Opfer in Kontakt zu treten. Aus diesem Grund wird im Rahmen der anstehenden Überarbeitung der Kataloge in dem speziellen Deliktsbereich eine entsprechende Bereinigung vorgenommen. Daneben wird die Verknüpfung der bisherigen Katalogbegriffe in den bereits existierenden Datensätzen anlassbezogen gelöscht.

Besondere Kategorien personenbezogener Daten – z. B. über das Sexualleben von Opfern oder Tatverdächtigen – dürfen nur dann in polizeilichen Informationssystemen gespeichert werden, wenn dies für die Ermittlungstätigkeit zwingend erforderlich ist.

Löschprüffristen für ed-Unterlagen in INPOL-Dateien

Der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich wiederholt – zuletzt im Zusammenhang mit der Einführung von INPOL-neu – mit der Praxis der Speicherung von Daten über die erkennungsdienstliche Behandlung von Personen (ed-Unterlagen) bei dem Bundeskriminalamt (BKA) beschäftigt. Dabei ging es u. a. darum, worauf es zurückzuführen ist, dass die bei dem BKA noch gespeicherten Daten im Landesbestand der jeweils einstellenden Polizeibehörde längst gelöscht und die dazugehörigen Unterlagen vernichtet sind, also warum unterschiedliche Löschprüffristen festgelegt sind.

In den Verbunddateien „Erkennungsdienst“ und „*AFIS“ („Automatisiertes Fingerabdruck-Identifizierungssystem*“) werden alle Betroffenen einer erkennungsdienstlichen Behandlung durch Abnahme der Fingerabdrücke, zu denen eine Kriminalakte vorliegt, bei dem BKA erfasst. Das geschieht einerseits in der Datei „Erkennungsdienst“ – dort werden die Ident-Daten der Betroffenen sowie die Vorgangsdaten gespeichert – und andererseits in der Datei „AFIS“, wo die verformelten Finger- und Handflächenabdrücke sowie die entsprechenden Spuren gespeichert sind. Dabei kann der Zugriff sowohl über die Ident-Daten der Betroffenen als auch über die Abdrücke erfolgen. Die Dateneingabe in Verbunddaten richtet sich nach dem Bundeskriminalamt-Gesetz (BKAG). Nach § 2 Abs. 4 BKAG unterhält das BKA zentrale erkennungsdienstliche Einrichtungen und Sammlungen zur Unterstützung der Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten und bei der Gefahrenabwehr. Auf die sonst erforderliche länderübergreifende, internationale oder sonst erhebliche Bedeutung (§ 2 Abs. 1 BKAG) kommt es dabei nicht an. Das BKA kann Daten, die bei der Durchführung von ed-Maßnahmen erhoben wurden, über Beschuldigte oder Verdächtige jeder Straftat verarbeiten, wenn eine andere Rechtsvorschrift das erlaubt oder dies erforderlich ist, weil bei Beschuldigten und Tatverdächtigen wegen der Art der Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstigen Erkenntnissen Grund zu der Annahme besteht, dass gegen ihn Strafverfahren zu führen sind, oder zur Abwehr erheblicher von ihm ausgehender Gefahren (§ 8 Abs. 6 BKAG). Es ist also eine Negativ-Prognose für den Betroffenen erforderlich.

Die Verbundteilnehmer – also die Polizeien des Bundes und der Länder – übermitteln dem BKA als Zentralstelle die zur Erfüllung seiner Aufgabe erforderlichen Informationen. Nur der Verbund-teilnehmer, der einen Datensatz eingegeben hat, ist befugt, diesen zu ändern, zu berichtigen oder zu löschen (§ 11 Abs. 3 BKAG). Weiterhin ist er zu informieren, wenn ein anderer Verbundteilnehmer feststellt, dass das Datum unrichtig ist. Die einstellende Polizei ist verpflichtet, diese Mitteilung unverzüglich zu prüfen und erforderlichenfalls die Daten unverzüglich zu ändern, zu berichtigen oder zu löschen. Darüber hinaus kann jeder Verbundteilnehmer des polizeilichen Informationssystems weitere Daten ergänzend eingeben, sofern bereits ein Datensatz existiert. Die datenschutzrechtliche Verantwortung trägt nach § 12 Abs. 2 BKAG die unmittelbar eingebende Stelle für die von ihr

eingegebenen Daten. In der Datei muss die verantwortliche Stelle erkennbar sein. Die anliefernde Stelle teilt bei der Übermittlung von personenbezogenen Daten an das BKA als Zentralstelle außerhalb des polizeilichen Informationssystems die nach ihrem Recht geltenden Löschungsverpflichtungen mit (§ 32 Abs. 7 BKAG). Das BKA hat diese einzuhalten. Die Löschung unterbleibt nur, wenn Anhaltspunkte dafür bestehen, dass diese Daten für das BKA als Zentralstelle – namentlich bei Vorliegen weitergehender Erkenntnisse – erforderlich sind, es sei denn, auch das BKA wäre zur Löschung verpflichtet. Es ist allerdings erforderlich, dies im Einzelfall zu prüfen (§ 32 Abs. 3 BKAG).

Der Arbeitskreis Sicherheit ist sich in der rechtlichen Beurteilung einig, dass für die Daten aus ed-Behandlungen das jeweilige Landesrecht der anliefernden Polizeibehörde Anwendung findet. Der Bundesbeauftragte für den Datenschutz wurde gebeten, die Problematik beim BKA weiterzuverfolgen.

Das Bundeskriminalamt hat als Zentralstelle in Verbunddateien die verkürzten Prüf- und Löschfristen zu beachten, die für die anliefernden Landespolizeien gelten.

Eine ungenehmigte Nebentätigkeit und deren Folgen

Eine Polizeibeamtin auf Probe hat in einem Lokal als Tresenkraft gearbeitet. Der Polizeipräsident in Berlin hat ein Verbot der Amtsausübung ausgesprochen und das mit den Ergebnissen einer von der Staatsanwaltschaft bei dem Landgericht Berlin durchgeführten Telefonüberwachung im Rahmen eines strafrechtlichen Ermittlungsverfahrens wegen des Verdachtes der gewerbsmäßigen Einschleusung sowie der Zuhälterei begründet. Danach sei die Polizeibeamtin in dem von dem Hauptbeschuldigten betriebenen Lokal einer nicht genehmigten Nebentätigkeit nachgegangen. Dabei soll sie Umgang mit Personen gepflegt haben, die offensichtlich der Organisierten Kriminalität zuzurechnen seien. Darüber hinaus soll sie durch die Weitergabe von dienstlich gewonnenen Erkenntnissen das Dienstgeheimnis verletzt haben.

Die Polizeibeamtin hat eingeräumt, die bezeichneten Personen persönlich zu kennen; sie hat aber zu keinem Zeitpunkt davon Kenntnis gehabt, dass diese Aktivitäten im Sinne einer Organisierten Kriminalität entfaltet hätten.

Aus der Akte hat sich ergeben, dass die Ermittlungsdienststelle des Landeskriminalamtes detaillierte Akteninhalte aus dem Strafermittlungsverfahren an die Personalakten führende Stelle übermittelt hat. Dabei hat es sich um zusammenfassende Ermittlungsvermerke, insbesondere um zusammengefasste Telefonabhörprotokolle der im Rahmen des Ermittlungsverfahrens durchgeführten Telefonüberwachungsmaßnahmen, gehandelt. Das Landeskriminalamt hat gegenüber der Personalstelle eine disziplinarrechtliche Überprüfung

angeregt. Das wurde damit begründet, dass die Polizeibeamtin regelmäßig telefonischen Kontakt zu tatbeteiligten Personen gehabt und selbst im Rahmen einer Nebentätigkeit in dem benannten Lokal als Tresenkraft gearbeitet hat. Durch die Telefonate mit ihrem Bekannten - dem Hauptbeschuldigten - habe ihr bewusst sein müssen, welcher Tätigkeit dieser nachgegangen ist.

Der Polizeipräsident in Berlin hielt das Vorgehen nach § 125 c Beamtenrechtsrahmengesetz (BRRG) für zulässig. Danach dürfen im Rahmen der Amtshilfe bei Strafverfahren sonstige Tatsachen, die in einem Strafverfahren bekannt werden, durch das Gericht, die Strafverfolgungs- oder Strafvollstreckungsbehörde dem Dienstherrn mitgeteilt werden, wenn ihre Kenntnis aufgrund besonderer Umstände des Einzelfalles für dienstrechtliche Maßnahmen gegen einen Beamten erforderlich ist und soweit nicht erkennbar schutzwürdige Belange des Beamten an dem Ausschluss der Übermittlung überwiegen. Der Polizeipräsident in Berlin vertritt weiterhin die Auffassung, dass die Übermittlung auch dann erforderlich ist, wenn diese Informationen lediglich Anlass zur Prüfung bieten, ob dienstrechtliche Maßnahmen zu ergreifen sind – also deren Notwendigkeit noch nicht feststeht. Die Staatsanwaltschaft bei dem Landgericht Berlin hat in dem gegen die Polizeibeamtin eingeleiteten strafrechtlichen Ermittlungsverfahren wegen versuchter Strafvereitelung abschließend festgestellt, dass die Erkenntnisse aus der Telefonüberwachung nicht verwertbar sind, und das Verfahren eingestellt.

Wir haben dem Polizeipräsidenten in Berlin dazu mitgeteilt, dass die genannte Vorschrift des BRRG zwar die Befugnis enthält, unter den dort genannten Voraussetzungen auch Erkenntnisse weiterzugeben; jedoch bedarf es neben der Abwägung mit schutzwürdigen Interessen der Polizeibeamtin an dem Ausschluss der Übermittlung zusätzlich der Berücksichtigung, wie gesichert die zu übermittelnden Erkenntnisse sind. Bei der Prüfung der Voraussetzungen des § 125 c Abs. 4 BRRG ist zu berücksichtigen, dass wegen der besonderen Gefährdung der Persönlichkeitsrechte der Betroffenen durch Mitteilungen aus einem Strafverfahren, das sich zudem nicht gegen die von der Mitteilung betroffenen Person selbst richtet, eine strenge Prüfung des Erforderlichkeitskriteriums vorzunehmen ist. Darüber hinaus ist zu prüfen, wie gesichert die zu übermittelnden Erkenntnisse sind. Diese Voraus-setzung ist von dem Landeskriminalamt nicht ausreichend geprüft worden. Die Tatsache, dass das gegen die Polizeibeamtin eingeleitete Ermittlungsverfahren wegen versuchter Strafvereitelung von der Staatsanwaltschaft bei dem Landgericht Berlin wegen Nichtver-wertbarkeit der Erkenntnisse aus den Maßnahmen der Telefonüberwachung eingestellt worden ist, lässt den Schluss zu, dass die Erkenntnisse nicht ausreichend gesichert i. S. d. § 125 c BRRG waren. Das Landeskriminalamt hätte vor der Datenübermittlung an die Personalakten führende Stelle diese Voraussetzungen sorgfältiger prüfen müssen. Aus diesem Grund war die Übermittlung der Daten unzulässig. Der Polizeipräsident in Berlin hat seine Dienststellen über das Ergebnis

informiert und sie aufgefordert, künftig vor der Übermittlung die rechtlichen Voraussetzungen sorgfältig zu prüfen.

Aus Strafverfahren gegen einen Beamten dürfen dem Dienstherrn nur gesicherte Erkenntnisse mitgeteilt werden, wenn dies für dienstrechtliche Maßnahmen erforderlich ist und weitere Voraussetzungen erfüllt sind.

Die Prominente und der *Personalausweis*

> *Die Berliner Polizei hat die in einem Artikel einer Schweizer Illustrierten veröffentlichte Vorderseite des Personalausweises einer prominenten Schauspielerin verwendet, um in einem völlig anderen strafrechtlichen Ermittlungsverfahren gegen den Betreiber einer Internetseite, mit dem sie in keiner Verbindung steht, ein dort verwendetes Sicherheitssystem, das den Zugang Minderjähriger verhindern soll, zu überprüfen. Die Schauspielerin hat das Land Berlin auf Schadensersatz wegen Verletzung ihres Persönlichkeitsrechts verklagt. Ihre Klage wurde jedoch vom Landgericht Berlin abgewiesen.*

Die Polizei hält ihr Vorgehen für zulässig. Nach der Strafprozessordnung gilt für die Polizei und die Staatsanwaltschaft der Grundsatz der freien Gestaltung des Ermittlungsverfahrens (§ 163 Abs. 1 StPO). Aufgrund dieser Generalklausel ist die Polizei zu solchen Eingriffen ermächtigt, die in ihrer Eingriffsintensität hinter den gesetzlich geregelten zurückbleiben. Das ist hier der Fall. Zum Nachweis, wie einfach es für Minderjährige ist, an fremde Personalausweis-daten zu gelangen, nahm der Ermittlungsbeamte die Kopie eines Artikels einer Schweizer Illustrierten zur Ermittlungsakte, in dem die Schauspielerin ihren Personalausweis abbilden ließ. Bei den darin enthaltenen Daten handelt es sich um offenkundige, d. h. allgemein zugängliche Daten. So auch bei der Personalausweisnummer, die zur Überprüfung des Entschlüsselungs-programms verwendet wurde. Auch das Landgericht kommt in seiner Urteilsbegründung[55] zu dem Schluss, dass der Anspruch auf Schutz der veröffentlichten Daten aufgegeben wurde. Es führt in diesem Zusammenhang aus, die Klägerin sei eine dem breiten Publikum bekannte Person, die die Öffentlichkeit nicht scheut, wie sich hier auch an dem in der Schweizer Illustrierten veröffentlichten Artikel manifestiert. Wer aber seine Privatsphäre in bestimmten Bereichen der Öffentlichkeit zugänglich macht, könne sich nicht gleichzeitig auf den von der Öffentlichkeit abgewandten Privatsphärenschutz berufen.

Von der zivilrechtlichen Frage, ob der Schauspielerin Schadensersatz und Schmerzensgeld

55 Urteil v. 26. Juli 2006 – 270301/05

zusteht, ist die Frage zu unterscheiden, ob die Polizei durch ihr Vorgehen in diesem Fall Datenschutzrecht verletzt hat. Nur diese zweite Frage, die das Landgericht offen gelassen hat, hatten wir zu beurteilen und wir haben sie bejaht.

Ein Verstoß gegen das Datenschutzgesetz liegt nicht erst bei einer schwer wiegenden Persönlichkeitsrechtsverletzung und einem schweren Verschulden der verantwortlichen Stelle vor, wie sie das Zivilrecht für einen Anspruch auf Schmerzensgeld voraussetzt.

Es ist zwar zutreffend, dass der Grundsatz der freien Gestaltung des Ermittlungsverfahrens auch für die Polizei gilt. Allerdings sind hierbei die sich aus der Verfassung ergebenen Grenzen zu beachten. Aus dem Grundsatz der Verhältnismäßigkeit ergibt sich, dass eine Grundrechte beschränkende Maßnahme (hier: die Nutzung eines personenbezogenen Datums) unter Würdigung aller persönlichen und tatsächlichen Umstände des Einzelfalls zur Erreichung des angestrebten Zwecks geeignet und erforderlich sein muss. Das ist dann nicht der Fall, wenn ein milderes Mittel ausreicht und der damit verbundene Eingriff nicht außer Verhältnis zur Bedeutung der Sache und zur Stärke des bestehenden Tatverdachts steht. Sofern – wie im vorliegenden Fall – personenbezogene Daten Dritter verwendet werden, sind die Anforderungen an die Verhältnismäßigkeit besonders streng auszulegen.

Unabhängig davon, ob es sich um Daten handelt, die allgemein zugänglichen Quellen entnommen wurden oder nicht, ist hier entscheidend, dass diese Daten durch die Verwendung in einem Ermittlungsverfahren, das die Schauspielerin in keiner Weise berührt, in einen ganz neuen Sachzusammenhang gestellt wurden. Es wird ein Zusammenhang zwischen der Schauspielerin und dem geführten Ermittlungsverfahren hergestellt. Ob das für die Durchsetzung des zivilrechtlichen Schadensersatzanspruches ausreicht oder nicht, ist in diesem Zusammenhang ohne Belang. Die Verwendung der Daten aus dem Personalausweis ist jedoch für die Ermittlungen gerade nicht erforderlich. Vielmehr hätten für die Ermittlungen auch Daten anderer Personen – selbstverständlich mit deren Einwilligung – verwendet werden können. Der Zweck hätte auch mit anderen Daten erreicht werden können. Minderjährige haben mitunter auch Zugriff auf die Personalausweise ihrer Eltern oder Verwandten, so dass es der Verwendung der veröffentlichten Daten einer prominenten Person nicht bedurfte, um die mangelnde Effektivität von Jugendschutzmaßnahmen zu belegen.

Auch veröffentlichte Daten prominenter (oder nicht prominenter) Personen dürfen nur nach Maßgabe datenschutzrechtlicher Bestimmungen von öffentlichen Stellen, z. B. der Polizei, genutzt werden.

4.1.2 Verfassungsschutz

***Akkreditierungsverfahren* im Rahmen der *Fußball-Weltmeisterschaft 2006* – „Die Welt zu Gast bei Freunden“?**

In der Bundesrepublik Deutschland wird im Jahr 2006 die Fußball-Weltmeisterschaft stattfinden. An der Durchführung dieser Veranstaltung werden etwa 250.000 Menschen aus den ver-schiedensten Bereichen und Branchen beteiligt sein und Zutritt zu bestimmten, nicht-öffentlichen Bereichen der Stadien erhalten. Sie sollen in einem Akkreditierungsverfahren auf ihre Zuverlässigkeit hin überprüft werden. Betroffen sind nicht nur Journalisten, Fußballspieler und Sicherheitspersonal, sondern auch Mitarbeiter von Hilfsorganisationen und Sanitäts-diensten oder des gastronomischen Bereiches, Reinigungskräfte, Begleitpersonal sowie andere Servicebedienstete aller Sparten. Hierbei ist eine umfassende Beteiligung aller Sicherheits-behörden vorgesehen, die ihre Datenbestände zu den betroffenen Personen abgleichen sollen. Sowohl das *Landeskriminalamt* als auch der *Verfassungsschutz* sollen ein Votum zu den jeweiligen Personen abgeben.

Über die Akkreditierung wird ein Organisationskomitee (OK FIFA WM 2006) des Deutschen Fußballbundes (DFB) entscheiden, das sich auch auf ein Votum des *Bundeskriminalamtes* (BKA) stützt. Die Entscheidung des BKA wiederum beruht neben eigenen Erkenntnissen auf den Stellungnahmen der weiteren zu beteiligenden Stellen, also auch des Landeskriminalamtes und des Verfassungsschutzes. Beim Confederations Cup 2005, dem Probelauf für die WM 2006, war allein die Polizei an einem entsprechenden Akkreditierungsverfahren beteiligt.

Eingeleitet wird das Akkreditierungsverfahren für die WM 2006 bei freiberuflich Tätigen und Selbständigen, indem diese bei dem Organisationskomitee (OK) einen Antrag auf Zulassung stellen. Bei Arbeitnehmern stellt in der Regel der jeweilige Arbeitgeber in Form von Sammel-Akkreditierungen für seine Mitarbeiter den Antrag. Den Betroffenen soll zuvor eine Datenschutz-information ausgehändigt werden. In einem zweiten Schritt geben die Betroffenen eine Einwil-ligungserklärung zur Durchführung des Akkreditierungsverfahrens ab. Arbeitnehmer tun dies gegenüber ihrem Arbeitgeber.

Das OK will das Verfahren ausschließlich online abwickeln; die personenbezogenen Informationen werden also ausschließlich über das Internet übermittelt. Eine Weitergabe der Einwilligungs-erklärung im Original an die Sicherheitsbehörden ist nicht vorgesehen. Eine elektronische Authentifizierung erfolgt. Das OK übermittelt den Sicherheitsbehörden aber nur die zur Durchführung des Akkreditierungsverfahrens bestimmten Informationen über die zu akkreditierenden Personen. Das BKA erhält als einheitliche Anlaufstelle (Technical Single Point of Contact) vom OK den Gesamtdatenbestand; die Landeskriminalämter erhalten vom BKA die Daten

zu den Personen, die ihren Wohnsitz im jeweiligen Bundesland haben. Auch die Verfassungsschutzbehörden erhalten vom BKA die Daten zum Abgleich mit ihren Dateien. Die Landeskriminalämter geben ein Gesamt-Votum ab, ob gegen die Akkreditierung der jeweiligen Person Bedenken bestehen. Hierin fließen die bei dem Landeskriminalamt über die jeweilige Person gespeicherten Erkenntnisse und das Votum des BKA ein. Ist eines der Voten negativ, so fällt das Gesamt-Votum ebenfalls negativ aus. Die Verfassungsschutzbehörden des Bundes und der Länder bilden aus den bei ihnen vorhandenen Informationen ebenfalls Voten. Das Bundesamt für Verfassungsschutz fasst die einzelnen Voten zu einem Gesamt-Votum zusammen und übermittelt dieses an das BKA. Die Voten der Landeskriminalämter und der Verfassungsschutzbehörden erhält das BKA, das diese nicht an die Betroffenen, sondern vielmehr an das OK weiterleitet. Das OK übermittelt seine Entscheidung bei Sammel-Akkreditierungen dem jeweiligen Arbeitgeber des Betroffenen, bei Einzel-Akkreditierung dem Betroffenen selbst. In beiden Fällen teilt das OK aber lediglich mit, ob eine bestimmte Person akkreditiert wird oder nicht. Das OK teilt nicht mit, ob eine Akkreditierung aufgrund von Bedenken der Sicherheitsbehörden verweigert wird. Das OK hat sich in seinen Allgemeinen Geschäftsbedingungen vorbehalten, die Akkreditierung auch aus anderen Gründen (ohne Sicherheitsrelevanz) zu verweigern.

Die eingeschränkte Information durch das OK geht auf eine Vorgabe der örtlich zuständigen Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich (für den DFB ist dies das Regierungspräsidium Darmstadt) zurück. Auf diese Weise soll verhindert werden, dass ein Arbeitnehmer arbeitsrechtliche Nachteile erleidet, wenn ihm die Akkreditierung unter ausdrücklichem Hinweis auf Bedenken der Sicherheitsbehörden verweigert würde.

Die Ablehnungskriterien sind für Polizei- und Verfassungsschutzbehörden unterschiedlich ausgestaltet. Die Polizeibehörden entscheiden über die Akkreditierungsempfehlungen nach einem bundesweit geltenden Kriterienkatalog. Danach soll eine ablehnende Empfehlung an das OK abgegeben werden, wenn

- die überprüfte Person wegen einer Straftat mit erheblicher Bedeutung rechtskräftig verurteilt wurde; hierzu gehören insbesondere
  - Verbrechen,
  - Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie sich
    1. gegen das Leben, die Gesundheit oder die Freiheit einer oder mehrerer Personen oder bedeutende fremde Sach- oder Vermögenswerte richten oder
    2. auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- oder Wertzeichenfälschung oder des Staatsschutzes begangen werden oder

3. gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen werden;

- die überprüfte Person in der *Datei „Gewalttäter Sport*“ erfasst ist.

In Einzelfällen kann auch bei wiederholter Verurteilung oder wegen leichter Straftaten eine ablehnende Empfehlung gegeben werden. Sonstige Erkenntnisse – z. B. laufende oder eingestellte Ermittlungsverfahren oder Strafverfahren ohne gerichtliche Verurteilung – können zu einer ablehnenden Empfehlung führen, wenn dies nach einer sorgfältigen Prüfung des jeweiligen Falles angezeigt erscheint. Gleiches gilt, wenn über eine Person Staatsschutz-, Rauschgift- oder Erkenntnisse aus dem Bereich der Organisierten Kriminalität vorliegen, die darauf schließen lassen, dass sie künftig solche Straftaten begehen wird. Zur Erstellung einer Gefahrenprognose bedarf es in allen Fällen einer Würdigung aller polizeilich bekannten Erkenntnisse über den Antragsteller.

Die Verfassungsschutzbehörden sollen eine ablehnende Empfehlung nicht erst dann abgeben, wenn sich aus Erkenntnissen tatsächliche Anhaltspunkte ergeben, dass Personen Gewalttaten begehen werden, sie einer gewaltbereiten Bestrebung angehören oder ein vergleichbarer Fall vorliegt; vielmehr soll die ablehnende Empfehlung schon dann erfolgen, wenn aufgrund tatsächlicher Anhaltspunkte die Gefahr extremistischer Propaganda-Aktivitäten gesehen wird. Diese müssen nicht strafbar sein.

Das bundesweit vorgesehene Akkreditierungsverfahren kann zudem in Einzelfällen – trotz der beschriebenen eingeschränkten Information des Arbeitgebers durch das OK – zu einem Arbeitsplatzverlust der Betroffenen führen. Bei Journalisten ist die Presse- bzw. Rundfunkfreiheit betroffen. Für diesen Grundrechtseingriff gibt es keine gesetzliche Grundlage. Die Voraussetzungen für eine Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz liegen nach einhelliger Auffassung aller beteiligten Stellen nicht vor, da die Überprüfung weder dem Zweck des Geheim- noch des Sabotageschutzes dient. Die Zulässigkeit soll stattdessen allein auf die Einwilligung der Betroffenen gestützt werden. Problematisch dabei ist schon die Authentizität der Einwilligungserklärung. Die Sicherheitsbehörden sollen sich mit der allgemeinen Aussage des OK begnügen, der jeweilige Arbeitgeber habe ihm gegenüber durch einen Mausklick im Internet bestätigt, dass der Betroffene eingewilligt habe. Damit erhalten das Landeskriminalamt und der Verfassungsschutz keinen authentischen Nachweis, der die Urheberschaft der einwilligenden Personen sicherstellt. Lediglich der Arbeitgeber hat die schriftlichen Einwilligungserklärungen seiner Beschäftigten und soll sie bis zum Ablauf eines Vierteljahres nach dem Endspiel aufbewahren.

Voraussetzung einer wirksamen *Einwilligung* ist ihre Freiwilligkeit. Betroffen sind durch die Maßnahmen zahlreiche Arbeitnehmer, die auf Veranlassung ihrer jeweiligen Arbeitgeber

Tätigkeiten in den Stadionbereichen vorzunehmen haben. Die Betroffenen werden deshalb die Erklärung im Zweifel schon deshalb abgeben, um im Arbeitsverhältnis keine negativen Folgen, die mit der Ablehnung der Akkreditierung zusammenhängen, befürchten zu müssen. Freiwilligkeit setzt zudem das Wissen der Betroffenen über die Einzelheiten des Verfahrens sowie die Kenntnis voraus, über welche Daten sie im Einzelfall entscheiden. Der Betroffene kann schon deshalb keine ausreichende Kenntnis hiervon erlangen, weil das Konzept zur Beteiligung der Verfassungsschutzbehörden als „Verschlusssache“ eingestuft ist.

Für die ablehnende Empfehlung der Polizeibehörden des Bundes und der Länder soll das negative Votum eines einzelnen Landeskriminalamtes genügen. Die Behörde kann dieses Negativ-Votum auch auf Erkenntnisse über Staatsschutzdelikte stützen. Hierzu sind nach allgemeiner Praxis auch Propaganda-Delikte zu zählen. Eine generelle Einbeziehung solcher Delikte – ohne dass ein Bezug etwa zu Gewalttaten besteht – halten wir im Hinblick auf die Wahrung des rechtsstaatlichen Verhältnismäßigkeitsgebotes für zweifelhaft.

Noch zweifelhafter erscheint, dass die Verfassungsschutzbehörden überhaupt in das Akkreditierungsverfahren einbezogen werden und ihr Votum darauf stützen können, dass sie aufgrund tatsächlicher Anhaltspunkte die Gefahr extremistischer Propaganda-Aktivitäten sehen, die selbst jedoch nicht unbedingt strafbar sein müssen. Damit besteht die Möglichkeit, dass z. B. eine Reinigungskraft abgelehnt wird, die bei einer Verfassungsschutzbehörde wegen einer nicht strafbaren extremistischen Äußerung oder einer Mitgliedschaft bekannt ist. Die Ablehnungsentscheidung kann auf einer bloßen Verdachtslage beruhen.

Natürlich ist das Anliegen der Veranstalter und Sicherheitsbehörden berechtigt, einen störungsfreien und friedlichen Verlauf der Fußball-WM 2006 zu gewährleisten. Dabei handelt es sich jedoch um eine klassische Aufgabe der Polizei, nämlich die Abwehr von Gefahren für die öffentliche Sicherheit. Bezeichnenderweise nennt der DFB selbst das Akkreditierungsverfahren in der Einwilligungserklärung der Betroffenen eine „polizeiliche Zuverlässigkeitsprüfung“. Der Verfassungsschutz hat aber keine polizeilichen Aufgaben. Er kann nach den Verfassungsschutzgesetzen des Bundes und Berlins den Polizeibehörden lediglich Erkenntnisse übermitteln, wenn ihm Erkenntnisse über gewalttätige oder gewaltbereite Extremisten vorliegen. Es ist dagegen unverhältnismäßig, wenn zum Schutz auswärtiger Belange oder des Ansehens Deutschlands auch Erkenntnisse über nicht strafbare extremistische Aktivitäten einem ablehnenden Votum zugrunde gelegt werden können.

Die fehlende gesetzliche Aufgabenzuweisung für den Verfassungsschutz kann nicht durch eine Einwilligung der Betroffenen ersetzt werden. Dagegen erfüllt die Polizei im Rahmen des Akkreditierungsverfahrens eine Gefahrenabwehraufgabe. Ihre fehlende gesetzliche Befugnis zur

Datenverarbeitung in diesem Rahmen kann deshalb – im Gegensatz zur fehlenden Aufgabenzuweisung des Verfassungsschutzes – durch eine informierte Einwilligung der Betroffenen kompensiert werden.

In jedem Fall ist es für die von negativen Entscheidungen des OK Betroffenen schwer zu erkennen, aus welchen Gründen ihre Akkreditierung abgelehnt worden ist, und dementsprechend ihre Rechte auf Auskunft und ggf. Korrektur geltend zu machen. Zunächst müssen sie sich an das OK des DFB wenden, um herauszufinden, ob Sicherheitsbehörden Einwände gegen ihre Akkreditierung erhoben haben oder ob der DFB diese aus anderen Gründen verweigert hat. Wenn Sicherheitsbedenken bestehen, muss der Betroffene sich an das Landeskriminalamt seines Wohnsitzlandes wenden. Wenn die Sicherheitsbedenken nicht von diesem stammen, fragt es beim BKA als einheitlichem Kontaktpunkt an und leitet die Anfrage an das LKA weiter, das Einwände gegen die Akkreditierung erhoben hat.

Für die Betroffenen ist es zudem schwer zu erkennen, welche Stelle für die Datenverarbeitung verantwortlich ist. Nach außen tritt nur das BKA in Erscheinung. Im Falle von Auskunftsersuchen wird das BKA an das jeweilige Landeskriminalamt des Wohnsitzlandes verweisen. Vollends unübersichtlich wird die Situation für den Betroffenen, wenn ein Landesamt für Verfassungsschutz ein negatives Votum über ihn abgegeben hat. Das BKA weiß nicht, welches Landesamt dies ist, denn das Bundesamt für Verfassungsschutz gibt ihm gegenüber nur eine einheitliche Stellungnahme für alle Verfassungsschutzbehörden ab. Zugleich darf keine Polizeibehörde – auch nicht im Rahmen eines Auskunftsverfahrens – erfahren, dass über eine Person bei einer bestimmten Verfassungsschutzbehörde Erkenntnisse vorliegen (die diese nicht von sich aus der Polizei übermitteln dürfte). Der Bundesbeauftragte für Datenschutz und Informationsfreiheit hat sich beim Bundesministerium des Innern dafür eingesetzt, dass der Betroffene bei der Wahrnehmung seiner Rechte nach dem Datenschutzrecht einen einheitlichen Ansprechpartner erhält. Dabei wird auf eine Einhaltung des Trennungsprinzips zwischen Polizei und Nachrichtendiensten zu achten sein.

Die geschilderten Probleme der mangelnden *Transparenz* und der erschwerten Geltendmachung von Datenschutzrechten würden vermieden, wenn die Betroffenen von den Sicherheitsbehörden angehört werden, bevor das OK über sie eine ablehnendes Votum erhält. Dies würde dem Verfahren bei Auskünften aus dem Bundeszentralregister entsprechen.

Es wird dem Vernehmen nach auch von der Polizei in Nordrhein-Westfalen im Rahmen der Akkreditierung zur Fußball-WM angewandt.

Die Sicherstellung eines ungestörten und friedlichen Ablaufs der Fußball-WM 2006 ist eine Aufgabe der Polizei, nicht des Verfassungsschutzes. Nur die Datenverarbeitung der Polizei im Rahmen des

Akkreditierungsverfahrens ist durch eine informierte Einwilligung der Betroffenen zu rechtfertigen. Zur Geltendmachung von Auskunfts-, Korrektur- und Löschungsansprüchen müssen den Betroffenen ein zentraler Ansprechpartner zur Verfügung stehen und ein Mindestmaß an Transparenz gewährleistet werden.

4.2 Ordnungsverwaltung

4.2.1 Melde-, Personenstands- und Ausländerwesen

Übermittlung von Meldedaten zu Testzwecken an das Bundesministerium der Finanzen

> *Das Bundesamt der Finanzen teilt jedem Steuerpflichtigen zum Zweck der eindeutigen Identifizierung im Besteuerungsverfahren ein einheitliches, eindeutiges und dauerhaftes Merkmal (Identifikationsnummer) zu, das bei Anträgen, Erklärungen oder Mitteilungen gegenüber den Finanzbehörden anzugeben ist (§ 39 b Abgabenordnung). Es ist geplant, zum 1. Januar 2007 mit der Vergabe der Identifikationsnummern zu beginnen. Die Steueridentifikationsnummer wird dann im Melderegister gespeichert. Die Finanzminister des Bundes und der Länder haben am 3. März 2005 einstimmig beschlossen, diejenigen Länder, die zukünftig zu übermittelnde Daten bereits bereitstellen können, zu bitten, diese testweise für einen Probelauf dem Bundesamt der Finanzen zur Verfügung zu stellen. Ziel des Tests soll es sein, die Vergabe des Identifikationsmerkmals durch das Bundesamt der Finanzen an natürliche Personen zu beschleunigen. Nach Auffassung der Finanzverwaltung kann nur durch einen Test mit Echtdaten die Größenordnung der festgestellten und aufzuklärenden Dubletten ermessen werden.*

Zu den neu geschaffenen gesetzlichen Regelungen im Bereich der Finanzverwaltung haben wir uns bereits geäußert[56]. Die testweise Übermittlung von echten Meldedaten halten wir für unzulässig. Die Übermittlung der Meldedaten kann erst ab dem Zeitpunkt der Einführung des Identifikationsmerkmals erfolgen, der durch Rechtsverordnung von der Bundesregierung mit Zustimmung des Bundesrates bestimmt wird. Es ist kein zwingender Grund erkennbar oder gar geltend gemacht worden, der einen Vorgriff auf die Rechtsverordnung rechtfertigen würde. Ohne diese Rechtsverordnung würde es sich um eine zweckfremde Datenübermittlung handeln. Ein Ausnahmefall in Anlehnung an den Rechtsgedanken des § 11 Berliner Datenschutzgesetz (BlnDSG) liegt hier nicht vor. Zwar hatte das Bundesministerium der Finanzen signalisiert, dass die Bundesregierung noch 2005 eine Rechtsverordnung erlassen wollte, in der auch Regelungen zum Testverfahren aufgenommen werden sollten. Dies ist

56 JB 2004, 3.2

jedoch nicht geschehen.

Ohne Rechtsgrundlage ist die Übermittlung echter Meldedaten zu Testzwecken unzulässig.

Das *automatisierte Abrufverfahren* für die BVG

> *Die BVG wollte in den Kreis der öffentlichen Stellen aufgenommen werden, die im Rahmen des automatisierten Abrufverfahrens nach der DVO-Meldegesetz Meldedaten abrufen dürfen. Damit sollte eine Identitätsprüfung der Fahrgäste vorgenommen werden können, die ohne gültigen Fahrausweis angetroffen wurden und sich nicht mit einem amtlichen Ausweispapier legitimieren konnten. Das würde gegenüber dem bisher praktizierten Verfahren – das Kontrollpersonal gibt die Personalien des Fahrgastes an den Leiter des Stützpunktes weiter, der seinerseits telefonisch beim Dauerdienst des damaligen Landeseinwohneramtes anfragt, ob mit diesen Daten eine Person in Berlin gemeldet ist, und informiert anschließend das Kontrollpersonal über das Ergebnis – längere Wartezeiten für alle Beteiligten erheblich verkürzen. Mit der Zugriffsmöglichkeit auf das Melderegister würde auch die Polizei entlastet, die nicht mehr so häufig zu Personalienfeststellungen gerufen würde.*

Nicht zuletzt deshalb, weil das Verfahren für eine Personenfeststellung ungeeignet ist, wurde die BVG nicht in den Kreis der abrufberechtigten Stellen der DVO-Meldegesetz aufgenommen. Auf diesem Wege kann lediglich festgestellt werden, ob in Berlin eine Person mit den angegebenen Daten gemeldet ist, nicht aber, ob die Person, die diese Angaben macht, identisch ist mit der im Melderegister gespeicherten Person.

Da Datenverarbeitung – dazu gehört auch der Abruf personenbezogener Daten im Rahmen von automatisierten Abrufverfahren (§ 4 Abs. 2 BlnDSG) – nicht nur aufgrund einer besonderen Rechtsvorschrift, sondern auch aufgrund der gleichberechtigten Alternative *„Einwilligung“* (§ 6 Abs. 1 BlnDSG) zulässig ist, wurde für die BVG ein Abrufverfahren auf freiwilliger Basis eingerichtet. Die betroffenen Fahrgäste willigen schriftlich in den Abruf ihrer Meldedaten durch die BVG ein. Die BVG ihrerseits muss den Nachweis dafür erbringen, dass für jeden getätigten Abruf auch eine solche Einwilligung vorliegt. Diese wohl in der Bundesrepublik Deutschland einmalige Einrichtung einer automatisierten Abrufmöglichkeit auf freiwilliger Basis ist auf ausdrücklichen Wunsch der BVG geschaffen worden. Wir haben unsere erheblichen Bedenken gegen die Geeignetheit des Verfahrens vor dem Hintergrund des Zieles, die Wartezeiten und Unannehmlichkeiten für die Fahrgäste erheblich zu reduzieren, zurückgestellt.

Bei einer Stichprobenuntersuchung von 25 Fällen anhand der protokollierten Abrufe konnten

uns allerdings in acht Fällen keine Einwilligungserklärungen vorgelegt werden. Die Originale wurden nicht aufgefunden. Die BVG führt das auf einen hohen Personalaufwand bei der Verwaltung der Einwilligungserklärungen zurück. Darüber hinaus sei trotz großer Sorgfalt nicht auszuschließen, dass einzelne Einwilligungen falsch abgelegt wurden. Weiterhin könne bei dem Kontrollpersonal nicht ausgeschlossen werden, dass es nicht immer mit der gebotenen Sorgfalt vorgegangen ist. Das ist nicht akzeptabel. Zur ordnungsgemäßen Datenverarbeitung gehört auch die sorgfältige Dokumentation. Im Übrigen geht es nicht um einige wenige Einzelfälle, sondern hier handelt es sich um eine erhebliche Größenordnung. Zwar hat die BVG das Kontrollpersonal nochmals belehrt. Ob das ausreicht, wird sich zeigen. Es wurden aber keine Maßnahmen zur Qualitätssicherung der Verwaltung bzw. der Ablage der Einwilligungserklärung getroffen. Hier besteht erheblicher Nachbesserungsbedarf. Dabei bietet sich beispielsweise eine unregelmäßige Stichprobenkontrolle durch den behördlichen Datenschutzbeauftragten an.

Weiterhin wurde der Probebetrieb mit Echtdaten durchgeführt. Dabei wurden die Daten ohne schriftliche Einverständniserklärung abgerufen. Diese Abrufe erfolgten also ebenfalls ohne Legitimationsgrundlage. Ferner liegen uns die erbetene Dateibeschreibung, die Risikoanalyse, das Sicherheitskonzept sowie ggf. das Ergebnis einer Vorabkontrolle der Datei „Namensmissbrauch“ sowie die Muster einer Einwilligungserklärung in die Speicherung in diese Datei trotz mehrerer Erinnerungen noch immer nicht vor. Das ist mit der Unterstützungspflicht nicht vereinbar (§ 28 BlnDSG).

Bei automatisierten Abrufverfahren aufgrund der Einwilligung der Betroffenen bestehen besondere Anforderungen an die zu treffenden technisch-organisatorischen Maßnahmen. Kann nicht für jeden protokollierten Abruf eine Einwilligungserklärung des Betroffenen vorgelegt werden, war der Abruf unzulässig.

Adoptionsgeheimnis

> *Empört haben sich die Eltern eines Adoptivkindes bei uns darüber beschwert, dass das Bezirksamt Charlottenburg-Wilmersdorf einer Privatperson die Namen der leiblichen Eltern und der Adoptiveltern des Kindes ohne Einwilligung der Betroffenen mitgeteilt hat.*

Hintergrund der Anfrage war ein von den Adoptiveltern angestrengtes Ermittlungsverfahren wegen falscher Verdächtigung, in dem die beim Standesamt anfragende Privatperson in Beweisnot geraten war. Aufgrund der Auskunft wurde das Ermittlungsverfahren eingestellt.

Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden können nur von den Behörden im Rahmen ihrer Zuständigkeit und von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen haben nur dann ein Recht auf Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden, wenn sie ein rechtliches Interesse glaubhaft machen. Grundsätzlich liegt das rechtliche Interesse einer Privatperson an der Einsicht bzw. Auskunft aus Personenstandsbüchern dann vor, wenn die Kenntnis der Personenstandsdaten eines anderen zur Durchsetzung von Rechten oder zur Abwehr von Ansprüchen erforderlich ist. Das ist hier der Fall; die Antragstellerin war in Beweisnot gegenüber der Staatsanwaltschaft geraten. Jedoch ist auch die zentrale Schutzvorschrift für angenommene Kinder, das Adoptionsgeheimnis zu achten (§ 1758 BGB). Danach ist eine Auskunft an Private – soweit es sich nicht um die Annehmenden, deren Eltern, den gesetzlichen Vertreter des Kindes und das über 16 Jahre alte Kind selbst handelt – unzulässig. Allerdings wäre die Offenbarung gegenüber der Staatsanwaltschaft auf entsprechende Anfrage zulässig gewesen.

Die Mitarbeiterin des Standesamtes hat den Fehler eingeräumt. Ihre Vorgesetzte ist zu dem Ergebnis gekommen, dass die Mitarbeiterin weder vorsätzlich noch grob fahrlässig gehandelt hat. Der Vorgang wurde zum Anlass genommen, die Mitarbeiterin auf die Probleme und insbesondere mögliche Folgen einer fehlerhaften Rechtsanwendung dieser Vorschrift hinzuweisen. Wir haben von einer förmlichen Beanstandung gegenüber dem Bezirksamt abgesehen, weil der Fehler sofort eingeräumt wurde.

Vor jeder Auskunft aus den Personenstandsbüchern ist sorgfältig die Zulässigkeit zu prüfen. Dies gilt in besonderem Maße bei Adoptionen.

***MESO* (Melde-, Ausweis- und Passregister)**

Mit MESO wurde das alte EWW-Verfahren abgelöst. Dabei handelt es sich um ein Standardprodukt. Es ist keine Individualsoftware für das Land Berlin, sondern musste den besonderen landesrechtlichen Regelungen (beispielsweise dem Berliner Meldegesetz) angepasst werden. Mit dieser neuen Software wird das Melde-, Pass- und Ausweisregister geführt.

Das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) hat uns dazu eine Dateibeschreibung für alle drei Register vorgelegt (§ 19 Abs. 2 BlnDSG). Bei den Aufgaben der Melde-, Ausweis- und Passbehörde handelt es sich um Ordnungsaufgaben mit der Folge, dass das ASOG anzuwenden ist (Nrn. 22 a, 33 der Anlage zum ASOG). Das suspendiert einerseits

die §§ 6 a, 9 Abs. 2 und 10 bis 17 BlnDSG (§ 51 ASOG) und schreibt andererseits vor (§ 49 Abs. 1 ASOG), dass u. a. für jede automatisierte Datei eine Errichtungsanordnung zu erlassen ist, die an die Stelle der Dateibeschreibung tritt (§ 19 Abs. 2 BlnDSG). Der Inhalt richtet sich nach den Dateirichtlinien. Somit ist für jedes Register eine gesonderte *Errichtungsanordnung* zu fertigen. Damit kann auch der Unübersichtlichkeit der vorgelegten Unterlagen entgegengewirkt werden. Die Unterlagen waren jedoch im Wesentlichen nicht prüffähig und erfüllten nur zum Teil die Anforderungen der Dateirichtlinien und des § 19 Abs. 2 BlnDSG. Selbst uns war es nur mit unverhältnismäßigem Aufwand möglich, die zu erfüllenden Aufgaben sowie die dabei verarbeiteten Daten mit den jeweiligen gesetzlichen Befugnisnormen und Aufgabenzuweisungsregelungen konkret in den notwendigen rechtlichen und tatsächlichen Zusammenhang zu bringen, um die Zulässigkeit der Datenverarbeitung zu überprüfen. Um den gesetzlich gebotenen Anforderungen zu entsprechen, sind die eingereichten Unterlagen im Hinblick auf diese gesetzliche Zielsetzung zu überarbeiten und dabei insbesondere folgende Verbesserungen anzubringen:

Bei der Verfahrensbeschreibung für das IT-Verfahren Einwohnerwesen werden listenförmig die maßgeblichen Verarbeitungsgrundlagen nach dem BlnDSG, dem Melde-, dem Ausweis-, dem Pass-, dem Personenstands- und Namensrecht, dem Staatsangehörigkeits-, dem Steuer-, dem Wahlrecht und nach sonstigen Vorschriften erwähnt. Die pauschale Angabe der Rechtsvorschriften reicht jedoch nicht aus, um die Aufgabenbefugnisse der Verfahrensbeschreibung „Bürgerservice“, „Listenerstellung“, „Statistiken“ und „Verzeichnisarbeit“ rechtlich nachvoll-ziehbar und bezogen auf die Aufgaben bzw. Befugnis darzustellen. Infolgedessen kann auch die dargestellte Aufgabe hinsichtlich der Zulässigkeit nicht geprüft und bewertet werden.

Die enthaltenen Angaben zur betroffenen Personengruppe und zu den diesbezüglichen Daten oder Datenkategorien sind bereichsspezifisch hinter den einzelnen Daten um die jeweilige Rechtsgrundlage zu ergänzen. Dies ist insbesondere deshalb erforderlich, weil über die in § 2 Abs. 1 Berliner Meldegesetz (MeldeG) enthaltenen Datengruppen hinaus auch weitere Daten verarbeitet werden, die dort nicht erwähnt sind, wie beispielsweise die Daten eines Lebenspartners. Entsprechendes gilt für das Ausweis- und Passregister. Die Empfänger oder Datenkategorien von Empfängern, denen die Daten mitgeteilt werden, sind zwar aufgelistet. Die Aufzählung dürfte aber nicht abschließend sein. Es sind offensichtlich die Empfänger regelmäßiger Datenübermittlungen nach der Nr. 4 der Anlage zu § 3 Nr. 1 DVO-MeldeG sowie der Ersten und Zweiten Bundesmeldedatenübermittlungsordnung (1. und 2. BMeldDÜV) aufgelistet. Der Hinweis auf Datenübermittlungen nach § 25 MeldeG fehlt völlig.

Unklar bleibt auch, ob sich die Aufstellung nur auf das Melde- oder auch auf das *Personalausweis- und Passregister* bezieht. Das wird dann später den getrennt für jedes Register zu

erlassenden Errichtungsanordnungen zu entnehmen sein. Auch bei der Herkunft regelmäßig empfangener Daten können rechtliche Überprüfungen nur vorgenommen und Transparenz nur dadurch hergestellt werden, wenn neben den absendenden Stellen auch die Daten selbst und die Rechtsgrundlage der Übermittlung dargestellt werden. Hinzu kommt, dass die Aufstellung unvollständig ist; es übermitteln beispielsweise nicht nur auswärtige, sondern auch Berliner Standesämter. Weiterhin werden zugriffsberechtigte Personen oder Personengruppen aufgezählt, die in der Anlage 5 zu § 3 Nr. 2 DVO-MeldeG enthalten sind. Diese Aufzählung ist nicht vollständig, weil die Stellen der Bezirksämter i. S. d. *funktionalen Behördenbegriffes* fehlen, denen über das „Portal Auskünfte für Behörden“ (PAB) der Zugriff eröffnet wurde bzw. wird. Erläuterungen zum Personalausweisregister fehlten ebenso wie die Angaben zur Art der Übermittlung (Nr. 3.10 der Dateienrichtlinien) völlig und sind in die für jedes Register zu fertigende Errichtungsanordnung einzuarbeiten.

Unsere Stellungnahme stammt aus dem Dezember 2004. Obwohl das Verfahren bereits im Echt-Betrieb läuft, liegen uns die überarbeiteten Errichtungsanordnungen noch immer nicht vor.

Für jede automatisierte Datei mit personenbezogenen Daten im Bereich der Ordnungsverwaltung ist jeweils eine aussagekräftige Errichtungsanordnung zu fertigen.

Diskretion im *Bürgeramt*

Immer wieder erreichen uns Beschwerden über die Möglichkeit des Mithörens der Gespräche nicht nur in *Jobcentern*[57], sondern auch in den Bürgerämtern[58]. Das Abgeordnetenhaus von Berlin hat in einem Beschluss den Senat aufgefordert, in den Bezirken darauf hinzuwirken, dass die Bürgerämter räumlich so ausgestaltet werden, dass die erforderliche Vertraulichkeit gewahrt bleibt[59]. Entgegen der Mitteilung zur Kenntnisnahme des Senats[60] hat es weitere oder erneute Probleme im Zusammenhang mit der Einhaltung der Diskretion in Berliner Bürgerämtern gegeben.

So hat sich eine Bürgerin darüber beschwert, dass sie bei der Beantragung einer Ausweisänderung im Bürgeramt Mahlsdorf an einem Arbeitsplatz bedient wurde, der direkt neben dem Bearbeitungsschalter der Kasse liegt. An diesem standen etwa fünf bis sieben andere Personen an und konnten dem Gespräch der Bürgerin mit der Sachbearbeiterin aufmerksam zuhören. Nachdem wir uns in die Sache eingeschaltet haben, hat das Bezirksamt zugesagt, bis Ende des

57 vgl. 3.2
58 JB 2003, 4.2.1
59 vgl. Anhang 1
60 Abghs.-Drs. 15/4148

Jahres 2005 Informationstresen einzurichten, mit denen eine hinreichende räumliche Trennung bei der Bearbeitung der Bürgeranliegen erreicht werden soll.

Dieser Fall war zum Zeitpunkt der Erstellung der Mitteilung des Senats, der eine aktuelle Befragung der Verantwortlichen der Bezirke vorausging, zumindest dem Bezirksamt bekannt. Im Übrigen hatten wir vom Senat anstelle allgemeiner Ausführungen über die Verantwortlichkeiten der Bezirksämter eine vergleichbare Unterstützung wie vom Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin erwartet. Dessen Vorsitzende hat den Parlamentsbeschluss den Vorstehern der Bezirksverordnetenversammlungen mit der Bitte übersandt, ihn in den jeweiligen Beratungsgremien zu berücksichtigen.

Die notwendige Diskretion ist gerade in Großraumbüros und Bürgerämtern, aber auch in allen anderen Verwaltungen und Publikumsverkehr sicherzustellen. Niemand muss es hinnehmen, dass Verwaltungsmitarbeiter sein Anliegen in Hörweite anderer Wartender mit ihm erörtern.

Ausländerregister

Im Oktober 2005 wurde das neue Datenverarbeitungsverfahren AusReg 2 zur Vorgangsbearbeitung eingeführt. Damit verbunden war die Übertragung der im Ausländerregister gespeicherten Daten auf eine veränderte Informationstechnik. Diese beiden Maßnahmen haben auf Art und Inhalt sowie Art und Gegenstand regelmäßiger Datenübermittlungen keinen Einfluss. Die sich aus dem Aufenthaltsgesetz ergebenden Änderungen sind berücksichtigt. Das Ausländerregister wird von der Ausländerbehörde zur Erfüllung der ihr nach dem Aufenthaltsgesetz, dem Asylverfahrensgesetz und den jeweiligen Nebenbestimmungen zugewiesenen Aufgaben geführt und besteht aus zwei Dateien. In die Ausländerdatei A werden die Daten von jedem Ausländer aufgenommen, der sich im Bezirk der Ausländerbehörde Berlin aufgehalten, bei ihr einen Antrag gestellt oder Einreise und Aufenthalt angezeigt hat und für und gegen den die Ausländerbehörde Berlin ausländerrechtliche Maßnahmen oder Entscheidungen getroffen hat. Die Ausländerdatei B enthält die Daten von Ausländern, die aus dem Bezirk der Ausländerbehörde Berlin fortgezogen oder verstorben sind.

Der vorgelegte Entwurf der Errichtungsanordnung enthielt im Wesentlichen vergleichbare Mängel wie oben zu MESO beschrieben. Die Ausländerbehörde hat die Errichtungsanordnung überarbeitet; sie entspricht jetzt den Anforderungen des ASOG (§ 49) und der dazu erlassenen Ausführungsvorschrift (Dateienrichtlinie). Die Risiko-Analyse muss noch ergänzt werden (§ 5

Abs. 3 BlnDSG).

Errichtungsanordnungen auch komplexer Datenverarbeitungsverfahren können transparent und prüffähig sein.

4.2.2 Verkehr

Die Ordnungsämter und die Überwachung des ruhenden Verkehrs

Mit dem Gesetz zur Errichtung bezirklicher *Ordnungsämter* ist die Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten im Bereich des ruhenden Verkehrs und deren Ahndung durch Verwarnungen auf die Bezirke verlagert worden. Die Bußgeldstelle verbleibt zentral bei dem Polizeipräsidenten in Berlin, der neben der Ahndung von Ordnungswidrigkeiten im fließenden Verkehr auch parallel neben den Bezirken weiterhin für die Verfolgung und Ahndung von Ordnungswidrigkeiten im ruhenden Verkehr zuständig bleibt. Die Dienstkräfte der bezirklichen Ordnungsämter überwachen den ruhenden Verkehr, stellen Verstöße gegen die straßenverkehrsrechtlichen Vorschriften für den ruhenden Verkehr, leiten Ordnungswidrigkeitenverfahren ein und ergreifen die gebotenen Gefahrenabwehrmaßnahmen (§ 2 Abs. 2 Ordnungsdiensteverordnung). Damit sind die bezirklichen Ordnungsämter also hinsichtlich des ruhenden Verkehrs Gefahrenabwehrbehörden. Auch hier besteht eine sachliche Doppelzuständigkeit für den Polizeipräsidenten in Berlin und die Ordnungsämter.

Offen geblieben sind in diesem Zusammenhang die Datenverarbeitungsbefugnisse. Der Polizeipräsident in Berlin konnte und kann im Rahmen des automatisierten Abrufverfahrens Daten aus dem *Zentralen Fahrzeugregister* abrufen. Diese Möglichkeit hatten die bezirklichen Ordnungsämter bisher nicht. Das Problem wurde so gelöst, dass die bezirklichen Ordnungsämter bei dem Polizeipräsidenten in Berlin nach den Halterdaten angefragt, dieser die Daten aus dem Zentralen Fahrzeugregister abgerufen und sie anschließend den bezirklichen Ordnungsämtern zur Verfügung gestellt hat.

Dieses Verfahren ist so unzulässig. Der Polizeipräsident in Berlin ist sowohl zuständige Verwaltungsbehörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten[61] als auch Gefahrenabwehrbehörde. Zu diesem Zweck darf er die erforderlichen Daten aus dem Zentralen Fahrzeugregister abrufen (§ 36 Abs. 2 StVG). Diese Erhebung von Daten muss jedoch für den Polizeipräsidenten in Berlin zur Aufgabenerfüllung in einem konkreten Einzelfall erforderlich sein. Diese Voraussetzung liegt aber dann nicht vor, wenn er die Daten für ein bezirkliches Ordnungsamt abruft, das sie dann in einem von ihm konkret zu bearbeitenden Einzelfall verwendet. Hier sind Doppelzuständigkeiten geschaffen worden, ohne dass die dafür erforderlichen Datenverarbeitungsbefugnisse den bezirklichen Ordnungsämtern eingeräumt wurden.

61 § 1 der Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten (ZustVO-OWiG)

Das Problem soll über den materiellen Polizeibegriff gelöst werden (§ 36 Abs. 2 StVG). Im Gegensatz zum formellen Polizeibegriff – der sich auf die Zuständigkeiten bezieht und alle Verwaltungsbehörden, die ausdrücklich als Polizei bezeichnet werden, erfasst – stellt der materielle Polizeibegriff alle Behörden, denen die Aufgaben der Gefahrenabwehr obliegen, mit der Polizei gleich. Danach durfte für die Ordnungsämter eine Abrufmöglichkeit geschaffen werden, weil sie auch Gefahrenabwehrbehörden sind (§ 2 Abs. 2 Ordnungsdienstever-ordnung).

Bei Aufgabenverlagerungen ist auch immer zu prüfen, ob die bestehenden Datenverarbeitungsbefugnisse ausreichend sind.

Eine Kundenliste für einen Parkplatz ...

> *Der Petent gibt an, dass er beim Bezirksamt Friedrichshain-Kreuzberg von Berlin, Abteilung für Stadtentwicklung und Bauen - Ordnungsamt – Straßenverkehrsbehörde, einen Antrag auf Erteilung einer Ausnahmegenehmigung zum Parken in der Parkraumbewirtschaftung nach der Straßenverkehrs-Ordnung (StVO) gestellt habe. Mit Schreiben vom 24. September 2004 habe das Ordnungsamt zur Ergänzung seiner Antragsunterlagen um Übersendung von weiteren Unterlagen gebeten. Insbesondere verlange das Ordnungsamt die Vorlage einer Kopie seines Mietvertrages und einen Nachweis über die Notwendigkeit der beantragten Parkraumbewirtschaftszonen, in dem er die Namen und Adressen seiner Kunden anzugeben habe.*

Das Ordnungsamt teilte mit, dass vor Erteilung einer Ausnahmegenehmigung zu prüfen sei, ob es sich bei dem Antragsteller überhaupt um ein Unternehmen handeln würde, das von seiner Aufgabenstellung und Größe eine derartige Ausnahmegenehmigung benötigt.

Der Petent sei nicht im Fernsprechbuch 2003/2004 (Gelbe Seiten) verzeichnet, auch ein Firmenbriefkopf tauche in den Akten nicht auf. Das Firmenfahrzeug, ein PKW, sei nicht auf die Firma, sondern auf eine bevollmächtigte Privatperson zugelassen. Daher seien die geforderten Nachweise über entsprechende Firmenaktivitäten für die ordnungsgemäße Antragsbearbeitung unentbehrlich. Da der Petent sein Gewerbe bisher nicht eindeutig nachgewiesen habe, sei die Vorlage der Gewerbeanmeldung erforderlich. Die Vorlage des Mietvertrages (nur erste und letzte Seite) diene als Nachweis dafür, dass ein Gewerbe nicht nur angemeldet worden sei, sondern auch betrieben werde. Da in dem Antragsverfahren auf Erteilung einer Ausnahme-genehmigung zum Parken in der Parkraumbewirtschaftung an den Nachweis der Antrags-voraussetzungen hohe Anforderungen zu stellen seien, sei darüber hinaus ein Nachweis des Petenten, dass dieser tatsächlich regelmäßig Kunden in den parkraumbewirtschafteten

Gebieten zu bedienen habe, erforderlich.

Nach § 18 Abs. 1 ASOG kann die Ordnungsbehörde zur Klärung des Sachverhalts in einer bestimmten ordnungsbehördlichen Angelegenheit Ermittlungen anstellen. Sie kann in diesem Zusammenhang personenbezogene Daten erheben, wenn das zur Erfüllung der ihr durch andere Rechtsvorschriften übertragenen Aufgaben erforderlich ist. Das Bezirksamt als Straßenverkehrsbehörde ist für die Befreiung von der Parkraumbewirtschaftung nach § 46 Abs. 1 Nr. 1 StVO zuständig und berechtigt, die zur Erteilung von Ausnahmegenehmigung erforderlichen Daten zu erheben.

Die Datenerhebung ist dann erforderlich, wenn im Einzelfall die Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden könnte und die Erhebung im Verhältnis zu dem angestrebten Zweck als angemessen erscheint. Die Erforderlichkeit der Datenerhebung durch Vorlage einer Kopie der Gewerbeanmeldung und des Mietvertrages (nur erste und letzte Seite) ist zu bejahen.

Nicht erforderlich und damit unzulässig ist jedoch die Erhebung von Daten Dritter in Form einer Liste mit Kundennamen und -adressen. Hier bestehen erhebliche Zweifel an der Geeignetheit der Datenerhebung zur Aufgabenerfüllung. Eine derartige Liste gibt nur eine Momentaufnahme der Kundenbeziehungen des Petenten wieder. Darüber, ob die Kundenbeziehungen bestehen bleiben und als Anlass für den Bedarf einer Ausnahmegenehmigung gewertet werden können, enthält die Liste keine Aussage. Die Erhebung der Kundendaten beim Petenten kann somit nicht auf § 18 Abs. 1 ASOG gestützt werden.

Sie widerspricht auch dem Polizeigesetz (§ 18 Abs. 4 ASOG). Danach sind Daten (hier die Daten über die Kunden) grundsätzlich bei den Betroffenen zu erheben. Ohne deren Kenntnis können Daten über Dritte nur unter den eingeschränkten Voraussetzungen des § 18 Abs. 4 Nr. 1–3 erhoben werden. Allerdings liegt hier keine der dort genannten Tatbestandsvoraussetzungen vor.

Die Anforderung einer Kopie der Gewerbeanmeldung und von Teilen des Mietvertrages im Rahmen der Parkraumbewirtschaftung ist datenschutzrechtlich nicht zu beanstanden. Datenschutzrechtlich unzulässig ist jedoch die Aufforderung zur Vorlage einer Liste mit den Kundennamen und -adressen. Dem Ordnungsamt wurde empfohlen, auf entsprechende Datenerhebungen zu verzichten.

4.3 Justiz

Neuerliche Ausweitung des „genetischen Fingerabdrucks“

Veranlasst durch Berichte über Fahndungserfolge mit dem genetischen Fingerabdruck, u. a. die schnelle Aufklärung des Mordes an dem Münchener Modeschöpfer Rudolph Moshammer, entbrannte im Berichtszeitraum eine erneute Diskussion um die Ausweitung des Instruments der DNA-Analyse im Strafverfahren.

Im Februar 2005 legten zunächst mehrere unionsregierte Bundesländer und schließlich die Fraktion der CDU/CSU einen Entwurf eines Gesetzes zur Neuregelung der DNA-Analyse zu Zwecken des Strafverfahrens vor[62]. Der Entwurf ging davon aus, dass die DNA-Analyse dem herkömmlichen Fingerabdruck gleichzusetzen ist. Auch der Richtervorbehalt sowie die materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sollten gestrichen werden. Außerdem sah der Entwurf einen Verzicht auf eine Prognose weiterer schwerer Straftaten (sog. Negativprognose) vor.

Die geplante Gleichsetzung von DNA-Analyse mit dem herkömmlichen Fingerabdruck wurde von den Datenschutzbeauftragten des Bundes und der Länder[63] scharf kritisiert. Bei einer Gleichsetzung der DNA-Analyse mit dem Fingerabdruck wird nämlich verkannt, dass es bereits nach dem derzeitigen Stand der Technik möglich ist, aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten) zu entnehmen. Welche zusätzlichen Erkenntnisse aufgrund des Fortschritts der Analysetechniken in Zukunft gewonnen werden können, ist derzeit nicht absehbar[64].

Der vorgelegte Gesetzentwurf scheiterte an den Stimmen der rot-grünen Koalition und der FDP. Allerdings legten die Koalitionsfraktionen kurze Zeit später selbst einen Gesetzentwurf vor, der eine erhebliche Ausweitung der DNA-Analyse vorsah.

Der Entwurf eines Gesetzes zur Novellierung der forensischen DNA-Analyse ist am 1. November 2005 in Kraft getreten[65]. Mit dem Gesetz wird die Schwelle für die Speicherung sensibler Informationen über immer mehr Betroffene in der zentralen Datei beim Bundes-

62 BR-Drs. 99/05; BT-Drs. 15/4926
63 Entschließung zwischen der 68. und 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 15. Februar 2005, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S.12
64 vgl. ebenda
65 BGBl. I 2005, 2360 ff.

kriminalamt im Vergleich zur bisherigen Gesetzeslage noch weiter herabgesetzt. Eine Entwicklung, die im Hinblick auf das informationelle Selbstbestimmungsrecht des Einzelnen verfassungsrechtlich sehr bedenklich ist. Im Folgenden werden nur einige der im Hinblick auf das Gesetz bestehenden Kritikpunkte benannt.

Bedenken bestehen im Hinblick auf die Regelung des Richtervorbehaltes. Auf den *Richter-vorbehalt* wird zwar nicht vollständig verzichtet, jedoch ist eine richterliche Entscheidung nach der Neufassung der §§ 81 f, g Strafprozessordnung (StPO) lediglich in denjenigen Fällen erforderlich, in denen der Betroffene nicht selbst seine Einwilligung erteilt. Diese Regelung begegnet erheblichen verfassungsrechtlichen Bedenken. An eine wirksame Einwilligung in die Erhebung hochsensibler persönlicher Informationen sind nämlich strenge Voraussetzungen zu stellen. Insbesondere kann die Einwilligung nur wirksam sein, wenn sie freiwillig ist. Ob von einer Freiwilligkeit der Einwilligung angesichts des besonderen psychischen Druckes, dem sich Beschuldigte in einem strafrechtlichen Ermittlungsverfahren oder verurteilte Straftäter, zu denen auch Strafgefangene gehören, regelmäßig ausgesetzt fühlen, die Rede sein kann, ist sehr fraglich. Die Zulässigkeit der DNA-Analyse setzt gemäß § 81 g StPO voraus, dass wegen der Art und Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen den Beschuldigten künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind (Negativprognose). Dies hat zur Folge, dass die Betroffenen bei Erteilung ihrer Einwilligung faktisch gezwungen werden, sich selbst eine Negativprognose auszustellen.

Nach § 81 g Abs. 1 Satz 2 StPO kann die wiederholte Begehung sonstiger (nicht erheblicher) Straftaten im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen. Diese Gleichsetzung ist ebenfalls verfassungsrechtlich problematisch. Völlig offen ist insbesondere, in welchen Fällen der Unrechtsgehalt einer Tat eine derartige Gleichsetzung rechtfertigt. Wie viele Straftaten das Kriterium der wiederholten Begehung erfüllen, ist ebenfalls unbestimmt. Vor diesem Hintergrund ist zu befürchten, dass es in der Praxis zu einer mit dem verfassungs-rechtlichen Grundsatz der Verhältnismäßigkeit unvereinbaren Ausdehnung der DNA-Analysen kommen wird.

Schließlich wurde durch Einfügung eines neuen § 81 h StPO eine gesetzliche Regelung für den Einsatz molekulargenetischer Reihenuntersuchungen auf Grundlage der Einwilligung der Betroffenen geschaffen. Es ist zwar zu begrüßen, dass der Gesetzgeber die Voraussetzungen molekulargenetischer Reihenuntersuchungen gesetzlich geregelt hat, leider fehlt es jedoch an einer Klarstellung im Gesetz, dass diese Maßnahme subsidiär zu anderen Ermittlungs-maßnahmen sein muss und lediglich als ultima ratio eingesetzt werden darf.

Es ist festzustellen, dass das im Gesetzentwurf genannte Ziel einer Verbesserung der rechtsstaatlichen Ausgestaltung des Verfahrens nicht erreicht worden ist. Vielmehr führen die Regelungen zu einer Verschlechterung der Rechte der Betroffenen bei der Anwendung des eingriffsintensiven Instituts der DNA-Analyse im Strafverfahren.

Neue gesetzliche Regelung für den *Großen Lauschangriff*

Nachdem das *Bundesverfassungsgericht* in seinem Urteil vom 3. März 2004 festgestellt hat, dass die den Großen Lauschangriff regelnden Vorschriften der Strafprozessordnung den Vorgaben des Artikels 13 Abs. 3 Grundgesetz (GG) nicht hinreichend Rechnung tragen und daher in wesentlichen Teilen verfassungswidrig sind, war der Bundesgesetzgeber aufgerufen, spätestens bis zum 30. Juni 2005 verfassungsgemäße Regelungen zu schaffen. Der Gesetzgeber musste insbesondere gesetzlich klarstellen, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf[66].

Der erste vom Bundesministerium der Justiz im Juni 2004 vorgelegte Referentenentwurf, der sich auf eine minimale Umsetzung der Vorgaben des Bundesverfassungsgerichts beschränkte und sogar das Abhören der Kommunikation mit Berufsgeheimnisträgern zuließ, wurde nach scharfer Kritik u. a. von Berufsverbänden und Datenschützern zurückgenommen[67]. Im September 2004 legte die Bundesregierung einen neuen Entwurf eines Gesetzes zur Neuregelung der *akustischen Wohnraumüberwachung* vor[68]. Der Entwurf verzichtete zwar auf Abhörbefugnisse für die Kommunikation im Rahmen beruflicher Verschwiegenheitsverhältnisse, ließ jedoch weiterhin offen, was unter dem Kernbereich privater Lebensgestaltung zu verstehen ist.

Nachdem der Bundesrat den Gesetzentwurf der Bundesregierung als unzureichend abgelehnt hatte, rief er den Vermittlungsausschuss an. Unter dem mit der Fristsetzung des Bundesverfassungsgerichts für eine Neuregelung bis zum 30. Juni 2005 verbundenen hohen Zeitdruck haben sich die rot-grüne Koalition und die CDU/CSU-Fraktion gegen die Stimmen der FDP im Vermittlungsausschuss auf einen Kompromiss geeinigt. Anderenfalls wäre die akustische Wohnraumüberwachung ab dem 1. Juli 2005 nicht mehr möglich gewesen. Ergebnis dieses Kompromisses ist ein gegenüber dem im Bundestag verabschiedeten Regierungsentwurf erweiterter Katalog der Anlasstaten für die akustische Wohnraumüberwachung.

66 dazu JB 2004, 4.3.1, S. 66 f.
67 JB 2004, 4.3.1, S. 66 f.
68 BR-Drs. 722/04

Nach Annahme des Gesetzentwurfs durch den Bundesrat am 16. Juni 2005 erfolgte einen Tag später die Zustimmung durch das Parlament. Rechtzeitig zum 1. Juli 2005 konnte das Gesetz in Kraft treten[69].

Die zentrale Vorschrift des § 100 c Strafprozessordnung (StPO) knüpft die Zulässigkeit des Abhörens und Aufzeichnens des in einer Wohnung nicht-öffentlich gesprochenen Wortes an den Verdacht einer besonders schweren Straftat, wenn diese auch im Einzelfall besonders schwer wiegt. § 100 c Abs. 2 StPO enthält einen umfangreichen abschließenden Katalog von Anlassdelikten. Hierbei handelt es sich um insgesamt mehr als sechzig unterschiedliche Delikte, die unterschiedlichen Gesetzen (z. B. Strafgesetzbuch, Kriegswaffenkontrollgesetz, Asylverfahrensgesetz, Aufenthaltsgesetz) zu entnehmen sind. Bei einigen der in diesem Katalog genannten Straftatbestände (z. B. Fälschung von Vordrucken für Euroschecks) muss die Frage nach der praktischen Relevanz erlaubt sein.

Um den Schutz des im Gesetz nicht näher definierten *Kernbereichs privater Lebensgestaltung* zu gewährleisten, hat der Gesetzgeber verschiedene Datenerhebungs- und Datenverwertungsverbote geschaffen. So ist das Abhören und Aufzeichnen unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Entsprechende Aufzeichnungen sind unverzüglich zu löschen. Erkenntnisse über solche Äußerungen dürfen nicht verwertet werden.

Obwohl der Gesetzgeber Vorschriften geschaffen hat, die die Anforderungen an die Datenverarbeitung regeln, ist es bedauerlich, dass er nach dem eindeutigen Urteil des Bundesverfassungsgerichts, das dem Abhören von Wohnungen enge Grenzen gesetzt hat, nicht ganz auf eine Neuregelung der massiv in die Privatsphäre der Betroffenen eingreifenden akustischen Wohnraumüberwachung verzichtet hat. Es bleibt zu hoffen, dass in der Praxis von der Möglichkeit der akustischen Wohnraumüberwachung restriktiv Gebrauch gemacht und in Zweifelsfällen im Interesse des Grundrechtsschutzes der Betroffenen auf diese Form der Überwachung verzichtet wird.

Zu bedenken ist außerdem, dass das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung weitreichende Auswirkungen auf andere *verdeckte Ermittlungsmaßnahmen* hat. Die von den Datenschutzbeauftragten aufgestellte Forderung, alle Formen der verdeckten Datenerhebung an den Maßstäben der Entscheidung zu messen und die Befugnisregelungen im repressiven wie im präventiven Bereich auf den Prüfstand zu stellen[70], gilt es

69 Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts v. 3. März 2004 (akustische Wohnraumüberwachung), BGBl. I 2005, 1841

70 vgl. Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der

auch auf Landesebene zügig umzusetzen.

Der Gesetzgeber muss nach der Rechtsprechung des Bundesverfassungsgerichts Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung auch im Polizei- und Verfassungsschutzrecht treffen.

Datenschutz in Rechtsanwaltskanzleien

> *Nach Auffassung der Berliner Rechtsanwaltskammer wie auch der Bundesrechts-anwaltskammer gilt das Bundesdatenschutzgesetz (BDSG) nicht für Rechtsanwälte. Deren Pflichten zum Umgang mit mandats- und nicht mandatsbezogenen Daten würden sich ausschließlich aus der Bundesrechtsanwaltsordnung (BRAO) ergeben. Für die datenschutzrechtliche Kontrolle der Rechtsanwälte sei nicht die Aufsichtsbehörde nach § 38 BDSG zuständig, sondern ausschließlich die jeweilige Rechtsanwaltskammer, deren Mitglied der Rechtsanwalt sei. Eine Kontrollkompetenz der Aufsichtsbehörde würde insbesondere die Verschwiegenheitspflicht des Rechtsanwalts nach § 43 a Abs. 2 BRAO tangieren.*

Diese Auffassung teilen wir nicht. Mit allen anderen Datenschutzaufsichtsbehörden in Deutschland vertreten wir die Auffassung, dass die Rechtsanwaltskammer schon aufgrund ihrer rechtlichen Struktur nicht als eine die Aufsichtsbehörde ersetzende datenschutzrechtliche Kontrollstelle in Betracht kommt. Nach § 62 Abs. 2 Satz 1 BRAO führt die Landesjustizverwaltung die Staatsaufsicht über die Rechtsanwaltskammer. Dies widerspricht Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie), wonach die Kontrollstellen die ihnen zugewiesenen Aufgaben in völliger *Unabhängigkeit* wahrnehmen. Der Bundesrechtsanwaltsordnung lässt sich nicht entnehmen, wie die Rechtsanwaltskammer die Verpflichtung, auch von Amts wegen ohne besonderen Anlass Prüfungen vorzunehmen, erfüllen will[71]. Die Rechtsanwaltskammern in Deutschland erfüllen auch nicht die Verpflichtung nach Artikel 28 Abs. 5 EG-Datenschutzrichtlinie, regelmäßig einen Bericht über ihre Datenschutztätigkeit zu veröffentlichen.

Es ist zwar zutreffend, dass die Rechtsanwaltskammer auch die Möglichkeit hat, aufgrund von

---

Länder v. 28./29. Oktober 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 15

71 vgl. insoweit Dammann, Ulrich; Simitis, Spiros: EG-Datenschutzrichtlinie, Art. 28, Rn. 4.8. Baden-Baden: Nomos Verlagsgesellschft, 1997

datenschutzrechtlichen Verstößen anwaltsrechtliche Maßnahmen zu ergreifen. Dies führt allerdings noch nicht dazu, dass die Rechtsanwaltskammer datenschutzrechtliche Kontrollbehörde ist. So kann etwa auch die Gewerbeaufsicht nach § 35 Gewerbeordnung (GewO) datenschutzrechtliche Sachverhalte würdigen, ohne dass dies zur Folge hat, dass die Gewerbeaufsicht als datenschutzrechtliche Aufsichtsbehörde angesehen werden kann. Insofern besteht kein Widerspruch darin, dass die Berufsaufsicht den gesamten Pflichtenkreis des Rechtsanwaltes umfasst, die Rechtsanwälte aber trotzdem nach § 38 BDSG unter der Aufsicht der datenschutzrechtlichen Aufsichtsbehörde stehen.

Hätte die Aufsichtsbehörde bei nicht mandatsbezogenen Daten in Anwaltskanzleien keine Kontrollkompetenz, würde dies dazu führen, dass sich Rechtsanwälte bei allen ihren wirtschaftlichen Aktivitäten der Kontrolle der Aufsichtsbehörde entziehen könnten, auch sonstige nicht-öffentliche Stellen könnten sich unter dem Dach einer Anwaltskanzlei einer Kontrolle nach § 38 BDSG entziehen. Dies würde zu einer deutlichen Schwächung des informationellen Selbstbestimmungsrechts führen, welches nach Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 Grundgesetz (GG) Verfassungsrang hat[72].

Das Bundesdatenschutzgesetz ist auf Rechtsanwälte auch hinsichtlich mandatsbezogener Daten anwendbar. Lediglich soweit bereichsspezifische Datenschutzvorschriften bestehen, treten die entsprechenden Vorschriften des Bundesdatenschutzgesetzes gemäß § 1 Abs. 3 Satz 1 BDSG zurück. Die punktuellen Regelungen in der Bundesrechtsanwaltsordnung (§ 43 a Abs. 2 Schweigepflicht, § 50 *Handakten*, §§ 56, 73 allgemeine Kontrollbefugnisse der Kammern wegen Berufsverstöße) bewirken nicht, dass das Bundesdatenschutzgesetz bei der mandatsbezogenen Informationsverarbeitung überhaupt nicht anwendbar ist.

Die Wahrung des - durch § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) strafrechtlich geschützten - *Berufsgeheimnisses* steht der Geltung des Bundesdatenschutzgesetzes und der Kontrolle durch die Aufsichtsbehörde nicht entgegen. § 1 Abs. 3 Satz 2 BDSG bestimmt lediglich, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleibt, d. h. dass sie neben den Bestimmungen des Bundesdatenschutzgesetzes zu beachten sind. Insbesondere gelten die Informationsrechte der Aufsichtsbehörden nach § 38 Abs. 4 i. V. m. § 24 Abs. 6 und 2 BDSG.

Teilweise wird die Auffassung vertreten, dass die Bundesrechtsanwaltsordnung und das Bundesdatenschutzgesetz nicht aufeinander abgestimmte Normkomplexe sind, so dass die Bundesrechtsanwaltsordnung in gewissem Umfang lückenhaft bliebe. Diese Lückenhaftigkeit sei allerdings analog dem Beschluss des *Bundesarbeitsgerichts* (BAG) vom 11. November

72 vgl. BVerfGE 65, 1

1997[73] hinzunehmen, ohne dass von dem in § 1 Abs. 3 BDSG konstituierten Subsidiaritätsprinzip, wonach die generelle Norm des Bundesdatenschutzgesetzes ohne weiteres Platz greift, wenn das bereichsspezifische Gesetz eine den Sachverhalt unmittelbar erfassende deckungsgleiche Regelung nicht enthält, Gebrauch zu machen ist. Es erscheint unwahrscheinlich, dass das BAG nach der Umsetzung der EG-Datenschutzrichtlinie die 1998 vertretene Rechtsauffassung aufrechterhalten würde. Die EG-Datenschutzrichtlinie schreibt nämlich vor, dass die verantwortlichen Stellen - so auch die Rechtsanwälte - bezüglich der Verarbeitung personenbezogener Daten von einer „völlig unabhängigen“ Instanz kontrolliert werden. Hätte der Gesetzgeber die Bundesrechtsanwaltskammer zur datenschutzrechtlichen Aufsichtsbehörde machen wollen, hätte er bei der Umsetzung der EG-Datenschutzrichtlinie die Bundesrechtsanwaltsordnung richtlinienkonform novelliert.

Gegen die Erstreckung der unabhängigen Datenschutzaufsicht auf mandatbezogene Informationen in Anwaltskanzleien ist eingewandt worden, durch eine Anrufung der Aufsichtsbehörde könnte ein Petent (z. B. ein gegnerischer Anwalt) den Kenntnisstand eines Rechtsanwalts ausspähen, indem er die Aufsichtsbehörde zu einer Prüfung der Kanzlei veranlasst. Auch könnten Strafverfolgungsbehörden auf die bei der Aufsichtsbehörde über einen Rechtsanwalt und seine Mandanten vorliegenden Informationen zugreifen, die der direkten Beschlagnahme entzogen seien. Dabei wird übersehen, dass der Berliner Beauftragte für Datenschutz und Informationsfreiheit auch als Aufsichtsbehörde verpflichtet ist, über die ihm amtlich bekannt gewordenen Tatsachen *Verschwiegenheit* zu wahren. Er darf ohne Genehmigung des Abgeordnetenhaus weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen über solche Angelegenheiten abgeben (§ 23 BlnDSG).

Für Rechtsanwaltskanzleien gilt grundsätzlich das Bundesdatenschutzgesetz. Sie unterliegen der Kontrolle der nach § 38 BDSG zuständigen Aufsichtsbehörde. Dies ist in Berlin nach § 33 Abs. 1 Berliner Datenschutzgesetz (BlnDSG) der Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Die folgenden drei Beispiele aus unserer Praxis machen deutlich, wie wichtig eine unabhängige Datenschutzaufsicht über *Rechtsanwälte* – nicht zuletzt im Interesse der Mandanten – ist.

Unberechtigter Abruf von Grundbuchauszügen aus dem maschinellen Grundbuch

73 1 ABR 21/97, NJW 1998, 2466 ff.

Ein Ehepaar wandte sich an uns und schilderte, im Rahmen eines Nachbarschaftsstreits habe ihr Nachbar durch seinen Rechtsanwalt Klage beim Amtsgericht erhoben. Der Rechtsanwalt habe dieser Klage einen Grundbuchauszug für das im Eigentum des Ehepaars stehende Grundstück beigefügt. Da ihr eigener Antrag auf Aushändigung eines Grundbuchauszuges für das Grundstück ihres Nachbarn wegen Fehlens eines berechtigten Interesses vom Grundbuchamt abgelehnt worden war, fragten sie sich, wie der Auszug in den Besitz des Rechtsanwalts ihres Nachbarn gelangen konnte, denn dort war das Vorliegen eines berechtigten Interesses ebenfalls zweifelhaft. Da der Rechtsanwalt gleichzeitig als Notar tätig ist, vermuteten sie, er habe den Grundbuch-auszug in dieser Funktion durch Abruf aus dem maschinell geführten Grundbuch erlangt. Diese Vermutung wurde durch die Präsidentin des Kammergerichts bestätigt.

Die Verwendung des automatisierten Abrufverfahrens für den Zweck, den Grundbuchauszug in einem gerichtlichen Verfahren als Rechtsanwalt zu verwenden, stellt in zweierlei Hinsicht einen Verstoß gegen datenschutzrechtliche Vorschriften dar.

Gemäß § 43 Abs. 2 Nr. 1 Bundesdatenschutzgesetz (BDSG) handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft. Das nach dieser Vorschrift erforderliche Merkmal des unbefugten Abrufs ist sowohl dann erfüllt, wenn der Täter abrufberechtigt ist und seine Befugnisse lediglich überschreitet, als auch in Fällen, in denen er sich unabhängig von einer Befugnis Zugang verschafft. Da im vorliegenden Fall eine Berechtigung zum Abruf für die Tätigkeit als Rechtsanwalt nicht ersichtlich war, haben wir einen Verstoß gegen die genannte Vorschrift angenommen.

Daneben liegt auch ein Verstoß gegen § 133 Abs. 6 Grundbuchordnung (GBO) vor. Nach dieser Vorschrift darf der Empfänger, soweit in dem automatisierten Abrufverfahren personenbezogene Daten übermittelt werden, diese nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt worden sind. Im konkreten Einzelfall war davon auszugehen, dass die in der Funktion als Notar erhaltenen personenbezogene Daten zweckwidrig für die Anwaltstätigkeit verwendet worden waren. Die Präsidentin des Kammergerichts hat den Rechtsanwalt auf die Unzulässigkeit derartiger Abrufe hingewiesen.

Wir haben dem betroffenen Rechtsanwalt unsere datenschutzrechtliche Bewertung dargelegt. Da uns der Rechtsanwalt daraufhin überzeugend mitteilte, es sei durch ein Versehen zu dem Abruf gekommen und er habe eine Arbeitsanweisung erlassen, um Sorge dafür zu tragen, dass sich derartige Vorfälle in Zukunft nicht wiederholen, haben wir davon abgesehen, ein Verfahren

nach dem Gesetz über Ordnungswidrigkeiten einzuleiten.

Der konkreten Eingabe lag sicherlich ein Einzelfall zugrunde, dennoch zeigen unsere Erfahrungen, dass es auch bei Rechtsanwälten besonders wichtig ist, ein Augenmerk auf die Einhaltung datenschutzrechtlicher Vorschriften durch diese Berufsgruppe zu richten.

Verweigerung von Auskünften durch einen Rechtsanwalt

> *Ein Bürger wandte sich an uns und beschwerte sich darüber, dass ein Rechtsanwalt einen Brief, der von dem Bürger selbst an seine Hausverwaltung gerichtet worden war, in einem Strafverfahren, in dem der Bürger als Zeuge geladen war, verlesen habe. Wir wurden um Aufklärung gebeten, wie der Rechtsanwalt in den Besitz dieses Briefes gelangen konnte.*

Der Rechtsanwalt berief sich auf unsere Aufforderung zur Stellungnahme hin auf seine *anwaltliche Verschwiegenheitspflicht* und teilte uns mit, er werde keine Auskunft zum Sachverhalt erteilen. Der Rechtsanwalt war auch nach einem umfangreichen Schriftwechsel, in dem wir ihm unsere Rechtsauffassung ausführlich dargelegt haben, nicht bereit, seiner Verpflichtung zur Auskunftserteilung nachzukommen.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist Aufsichtsbehörde gemäß
§ 38 Bundesdatenschutzgesetz (BDSG) und hat die Einhaltung datenschutzrechtlicher Vorschriften bei nicht-öffentlichen Stellen, zu denen auch die Rechtsanwälte gehören, zu kontrollieren.

Nach § 38 Abs. 3 BDSG haben die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1–3 der Zivilprozessordnung (ZPO) bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrig-keiten aussetzen würde. Die Wahrung des durch § 203 Abs. 1 Nr. 1 StGB strafrechtlich geschützten Berufsgeheimnisses steht der Geltung des BDSG dagegen nicht entgegen.

Insbesondere begründet die Offenlegung von Informationen aus dem *Mandatsverhältnis* kein *Auskunftsverweigerungsrecht* des Rechtsanwalts. Vielmehr erstreckt sich nach § 38 Abs. 4

Satz 3 i. V. m. § 24 Abs. 6 i. V. m. § 24 Abs. 2 Satz 1 Nr. 2 BDSG die Kontrollbefugnis der Datenschutzaufsichtsbehörden auch auf die einem Berufsgeheimnis unterliegenden personenbezogenen Daten.

Wir leiteten gegen den Rechtsanwalt ein Verfahren nach dem Gesetz über Ordnungs-widrigkeiten ein.

Rechtsanwälte sind der Aufsichtsbehörde gegenüber auch dann zur Auskunft verpflichtet, wenn es um Informationen aus dem Mandatsverhältnis geht. Sie können die Auskunft nur verweigern, wenn sie sich oder ihre Angehörigen dadurch der Gefahr eines Straf- oder Bußgeldverfahrens aussetzen.

Zweckentfremdung von *Halterdaten*

Ein Rechtsanwalt beantragte 1996 bei der Kfz-Zulassungsstelle im Landeseinwohner-amt eine Kfz-Halterauskunft. Dabei gab er an, dass die Anfrage im Zusammenhang mit einer Unfallangelegenheit stehe. Zur Durchsetzung der Ansprüche seines Mandanten würden Auskünfte aus dem Register zur Anschrift des Halters und zur Haftpflichtver-sicherung sowie der Versicherungsscheinnummer des schädigenden Fahrzeuges am Schadenstag benötigt. Tatsächlich war das angefragte Kfz nicht an einem Verkehrs-unfall am besagten Tag beteiligt. Ausweislich eines 2002 an das Amtsgericht Schöne-berg gerichteten Schreibens des Rechtsanwalts, mit dem das Gericht zugleich über die Haltereigenschaft der Petentin informiert wurde, diente die Halteranfrage einer Zwangsvollstreckung gegen die Petentin, die sich bei uns über das Vorgehen des Rechtsanwalts beschwerte.

Voraussetzung für die Halterauskunft nach § 39 Abs. 1 StVG ist, dass es dem Antragsteller um Rechtsansprüche im Zusammenhang mit dem Straßenverkehr geht. Die Erhebung der Halter-daten durch den Rechtsanwalt war rechtswidrig, weil die Daten zu einem anderen Zweck, nämlich zum Zweck der Zwangsvollstreckung, erlangt wurden. Deshalb war auch die Über-mittlung der durch die *Halteranfrage* erlangten Daten an das Amtsgericht Schöneberg 2002 rechtswidrig. Da der Rechtsanwalt sich uneinsichtig zeigte, haben wir ein Bußgeldverfahren wegen Verstoßes gegen § 43 Abs. 2 Nr. 1 BDSG eingeleitet. Danach handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Die 1996 erfolgte rechtswidrige Kfz-Halteranfrage konnte wegen der dreijährigen Verjährungsfrist nicht mehr verfolgt werden (§ 31 OWiG). Wegen der 2002 erfolgten rechtswidrigen Datenübermittlung an das Amtsgericht Schöneberg haben wir einen Bußgeldbescheid erlassen. Das Amtsgericht Tiergarten bestätigte unsere Auffassung, dass Fahrzeug- und Halterdaten, die im Rahmen der Halteranfrage nach § 39 Abs. 1 StVG übermittelt werden, nicht offenkundig und nicht allgemein zugänglich sind[74].

Die durch Kfz- Halteranfragen nach § 39 Abs. 1 StVG erlangten Daten sind – auch durch Rechtsanwälte – nur zu dem dort genannten Zweck zu verarbeiten.

74 vgl. auch Urteil des BGH v. 8. Oktober 2002, RDV 2003, 139 ff.

4.4 Finanzen

Auskunftsersuchen zur Grunderwerbssteuer

> *Das Finanzamt hat im Rahmen der Bemessung der Grunderwerbssteuer zu prüfen, ob ein sogenanntes einheitliches Vertragswerk über den Erwerb und die Bebauung eines Grundstücks oder eine andere Maßnahme (z. B. Abriss, Sanierung, Modernisierung) vorliegt, so dass neben dem Kaufpreis für den Grundbesitz auch andere Aufwendungen zur steuerlichen Bemessungsgrundlage gehören. Dazu erhebt das Finanzamt beim Steuerpflichtigen mit dem Fragebogen „Auskunftsersuchen zur Grunderwerbssteuer“ umfangreiche personenbezogene Daten. Unter anderem wird erfragt, wer die Finanzierung und den Notar vermittelt hat, wer bei der Beurkundung des Grundstücks-kaufvertrages anwesend war und wer bei der Beantwortung des Fragebogens mitgewirkt hat.*

Auch wenn die Regelungen der §§ 88 und 92 Abgabenordnung (AO) das Gebot der Normenklarheit, das vom Bundesverfassungsgericht für die Zulässigkeit der Einschränkung des Grundrechtes auf informationelle Selbstbestimmung verlangt wird, nur unzureichend erfüllen, kann die Datenerhebung des Finanzamtes mit dem Formular „Auskunftsersuchen zur Grunderwerbssteuer“ grundsätzlich auf diese Bestimmungen gestützt werden. Nach § 88 i. V. m. § 92 Satz 1 i. V. m. Satz 2 Nr. 1 AO kann sich die Finanzbehörde aller Beweismittel bedienen, welche sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält. Parallel dazu bestimmt § 9 Abs. 1 BlnDSG, dass die Datenerhebung nur dann zulässig ist, wenn sie zur rechtmäßigen Aufgabenerfüllung und für den damit verbundenen Zweck erforderlich ist.

Ein Kaufvertrag oder anderes Rechtsgeschäft, das den Anspruch auf eine Übereignung begründet, unterliegt nach § 1 Abs. 1 Satz 1 GrEStG der Grunderwerbssteuer. Bemessungsgrundlage ist nach § 8 Abs. 1 GrEStG der Wert der Gegenleistung. Nach § 9 Abs. 1 Satz 1 GrEStG gilt bei einem Kauf der Kaufpreis einschließlich der vom Käufer übernommenen sonstigen Leistungen als eine derartige Gegenleistung. Somit gehören zu der grunderwerbssteuerrechtlichen Gegenleistung (Bemessungsgrundlage) alle Leistungen des Erwerbers, die dieser nach den vertraglichen Vereinbarungen gewährt, um das Grundstück zu erwerben.

Steuerrechtlich von Bedeutung ist dabei die Tatsache, dass der Abschluss eines Werkvertrages zur Errichtung eines Gebäudes grundsätzlich nicht der Grunderwerbssteuer unterliegt. Jedoch können – wenn der Erwerbsvorgang insgesamt auf den Kauf eines Grundstückes mit Haus gerichtet ist – auch die Aufwendungen für den Hausbau zur Bemessungsgrundlage hinzugezählt werden. Dies führt dann zu rechtlich schwierigen Abgrenzungen, wenn ein Grundstück gekauft wird, jedoch erst später bebaut werden soll. Gegenstand der auf eine Grundstücks-

übereignung gerichteten Vereinbarung kann nach der Rechtsprechung des Bundesfinanzhofs sowohl das Grundstück in dem Zustand sein, den es zum Zeitpunkt des Vertragsschlusses hat, als auch in einem (künftigen) Zustand, in den es durch die Bebauung erst zu versetzen ist. Entscheidend ist in diesen Fällen, ob es sich bei dem Grundstückskaufvertrag und den Bau- und/oder Architektenverträgen um ein sog. „einheitliches Vertragswerk“ handelt. Ist dies zu bejahen, hat das zur Folge, dass der Erwerber das Grundstück in dem bebauten Zustand erwirbt, so dass auch die Bemessungsgrundlage für die Grunderwerbssteuer höher anzusetzen ist.

Sinn dieser rechtlichen Konstruktion ist es, die Steuerlast in den Fällen gleich zu verteilen, in denen das gleiche wirtschaftliche Ziel (Grundstück mit Bebauung) auf verschiedenen zivilrechtlichen Wegen (z. B. durch nacheinander oder mit verschiedenen Vertragspartnern abgeschlossene Verträge) erreicht werden soll.

Nach der Rechtsprechung wird der Gegenstand des Erwerbsvorganges um solche Vereinbarungen erweitert, die rechtlich oder wirtschaftlich in einem engen sachlichen Zusammenhang mit dem eigentlichen Grundstückserwerb stehen. Eine derartige Verknüpfung liegt jedenfalls dann vor, wenn die Verpflichtung zur Grundstücksübereignung und die Bauverpflichtung in einem Vertrag niedergelegt sind. Bei einer Aufspaltung in mehrere Verträge ist die Verknüpfung dennoch gegeben, wenn die Vereinbarungen nach dem Willen der Beteiligten auf ein entsprechend vergleichbares Ziel gerichtet sind.

Um einen einheitlichen Leistungsgegenstand kann es sich auch handeln, wenn der Erwerber bei objektiver Betrachtungsweise das bebaute Grundstück als Einheit erhält. Dies ist eine Einzelfallentscheidung und richtet sich danach, wieweit die Verträge verflochten sind oder ob die Vertragspartner des Erwerbers ihr Verhalten erkennbar aufeinander abgestimmt haben. Eine rechtliche Verknüpfung wird auch dann angenommen, wenn ein zwischengeschalteter Treuhänder die Beauftragung des Bauunternehmers erst noch übernehmen soll. Eine faktische Verbindung kann auch durch die Einschaltung eines Maklers entstehen, wenn dieser zugleich einen bestimmten Fertighausanbieter vertritt. Im Fall, dass der Bauerrichtungsvertrag erst nach Abschluss des Grundstückskaufvertrages abgeschlossen wird, wird ein enger sachlicher Zusammenhang je nach Ausgestaltung im Fall von faktischen Zwängen, vorherigen Absprachen oder der Hinnahme eines von der Veräußerungsseite vorbereiteten Geschehensablaufes angenommen.

Die Erforderlichkeit der einzelnen Fragen im Formular „Auskunftsersuchen zur Grunderwerbssteuer“ ist an den genannten Anforderungen der Rechtsprechung zu bemessen. Danach ist auch die Frage nach der Vermittlung der Finanzierung für die Ermittlung der

Bemessungsgrundlage grundsätzlich erforderlich. Die Ausgestaltung der Frage im Formular ist jedoch zu weitgehend. Es ist vielmehr konkret danach zu fragen, ob der Vertragspartner (Verkäufer/Bauunternehmer oder auch dessen Vertreter/Makler) die Finanzierung vermittelt habe. Andere Antwortalternativen sind als anonymisierte Fallgestaltungen (z. B. Steuerberater, Bekannte etc.) auszugestalten. Weitergehende personenbezogene Angaben über Dritte, die mit den Verträgen in keiner Verbindung stehen, sind nicht erforderlich und somit unzulässig. Dies gilt sinngemäß auch für die Fragen zur Vermittlung des Notars und zur Anwesenheit von Dritten bei der Beurkundung des Grundstückskaufvertrages. Dagegen ist die Frage danach, wer bei der Beantwortung des Fragebogens mitgewirkt habe, für die Ermittlung der Bemessungsgrundlage in keinem Fall erforderlich und damit unzulässig.

Die Senatsverwaltung für Finanzen hat angekündigt, den Fragebogen kritisch zu überprüfen. Jedenfalls werde in den Vordruck ein Hinweis aufgenommen, der allgemein über den Zweck der erbetenen Angaben und die Rechtsgrundlagen der Auskunftspflicht aufklärt.

Feststellung der Zugehörigkeit zu einer Religionsgemeinschaft

Mehrfach haben sich Bürger bei uns darüber beschwert, dass sie vom Finanzamt einen Fragebogen zur Klärung der Zugehörigkeit zu einer Religionsgemeinschaft erhalten hätten. Die Betroffenen wurden u.a. dazu befragt, ob sie Mitglied einer Kirche seien und, wenn dies nicht der Fall sein sollte, wann der Austritt erfolgt sei.

Nach dem Gesetz über die Erhebung von Steuern durch öffentlich-rechtliche Religionsgemeinschaften im Land Berlin (KiStG) können Kirchen und andere Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, Steuern aufgrund eigener Steuerordnungen erheben. Zu diesem Zweck haben die Katholische und Evangelische Kirche gemeinsame Kirchensteuerstellen eingerichtet, die zwar eng mit den Finanzämtern zusammenarbeiten und räumlich an diese angegliedert sind, rechtlich und organisatorisch jedoch zu den Kirchen gehören.

Während die Finanzämter die Berechnung der Kirchensteuer zusammen mit der Berechnung der übrigen Steuern durchführen, überprüfen diese Kirchensteuerstellen lediglich den Umstand, ob jemand durch Zugehörigkeit zu einer Religionsgemeinschaft kirchensteuerpflichtig ist. Eine Überprüfung ist dann notwendig, wenn ein Finanzamt von sich aus nicht ohne weiteres feststellen kann, ob eine Kirchenzugehörigkeit vorliegt oder nicht.

Das Recht der Kirchensteuerstellen zur Überprüfung der Religionszugehörigkeit ergibt sich aus Art. 140 GG in Verbindung mit Art. 136 Abs. 3 der Weimarer Reichsverfassung. Diese

Bestimmung der Weimarer Reichsverfassung ist aufgrund der Verweisung des Art. 140 GG Bestandteil des Grundgesetzes. Grundsätzlich ist danach niemand verpflichtet, seine religiöse Überzeugung zu offenbaren. Jedoch heißt es in Art. 136 Abs. 3 Satz 2 der Weimarer Reichsverfassung:

„Die Behörden haben nur soweit das Recht, nach der Zugehörigkeit zu einer Religionsgemeinschaft zu fragen, als davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert.“

Die Pflicht zur Zahlung der Kirchensteuer ist abhängig von der Religionszugehörigkeit. Demzufolge ist die Frage nach der Religionszugehörigkeit also zulässig. Die Religionszugehörigkeit hängt bei den christlichen Konfessionen von der Taufe ab.

Die Kirchensteuerstellen erhalten von den Finanzämtern an personenbezogenen Daten Steuernummer, Religionsmerkmal, Namen, Vornamen, Geburtsdatum, Anschrift sowie die Angabe, ab wann das Steuerkonto aufgenommen wurde. In der Regel wird sich anhand dieser Angaben die rechtliche Zugehörigkeit bzw. Nichtzugehörigkeit zur Evangelischen bzw. Katholischen Kirche feststellen lassen. Eine weitergehende Prüfung der Religionszugehörigkeit erfolgt nach Information des Datenschutzbeauftragten des Erzbistums Berlin nur in den Fällen, in denen Abweichungen zwischen vorliegender Grundinformation, Lohnsteuerkarte oder Angaben in der Steuererklärung auftreten. Der Fragebogen werde nur versandt, wenn die Zugehörigkeit zu einer Kirche nicht bereits eindeutig geklärt werden konnte. Hierbei ist problematisch, dass den Kirchensteuerstellen auch bei an sich eindeutigen Fällen die notwendigen Informationen nicht zur Verfügung stehen. Dies liegt zum Teil in dem fehlenden Abgleich zwischen kirchlichen Stellen und den Finanzämtern begründet (z. B. gibt ein Steuerpflichtiger nach einem Umzug gegenüber der Meldebehörde seine Kirchenzugehörigkeit nicht an, obwohl er tatsächlich nicht aus der Kirche ausgetreten ist), zum Teil in dem innerkirchlichen Organisationsaufbau. So werden die Daten über Kirchenmitglieder in der Gemeinde der Taufe geführt, nicht in der des Wohnsitzes. Die Kirchensteuerstellen haben danach nur die Möglichkeit, die Angaben durch den Fragebogen bei den Steuerpflichtigen selbst zu erheben.

Die Kontrollkompetenz des Berliner Beauftragten für Datenschutz und Informationsfreiheit erstreckt sich nach § 2 Abs. 1 BlnDSG nur auf die Behörden und öffentlichen Stellen des Landes Berlin. Daher sind – unabhängig von den vorstehenden allgemeinen Ausführungen – die Datenschutzbeauftragten der Evangelischen und Katholischen Kirche für die datenschutzrechtliche Prüfung des Inhalts des Fragebogens bzw. die Datenverarbeitung durch die Kirchen in Berlin zuständig.

4.5 Sozialordnung

4.5.1 Gesundheit

Elektronische Gesundheitskarte – Vorbereitungen in Berlin

Die bundesrechtlich festgelegte Einführung der elektronischen Gesundheitskarte für alle Versicherten der gesetzlichen Krankenversicherung ist sicherlich eines der größten IT-Projekte weltweit[75]. In einigen Modellregionen, zu denen Berlin nicht gehört, werden derzeit auf Grundlage einer Rechtsverordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte[76] Vorbereitungen zur Erprobung der verschiedenen Nutzungskomponenten getroffen. Diese Verordnung wurde vom Bundesministerium für Gesundheit erlassen, das damit in den Prozess der Selbstverwaltung eingreifen musste. Die für die Vorbereitung der Einführung gegründete Gesellschaft für Telematikanwendungen der Gesundheitskarte sah sich nicht in der Lage, im Konsens entsprechende Regelungen selbst zu treffen. In der Verordnung werden die einzelnen Testschritte festgeschrieben. Allerdings spiegelte der erste Entwurf der Verordnung nicht die Komplexität der Testung wieder, die erforderlich ist, um auch das Zusammenspiel der einzelnen Datenschutzmaßnahmen zu erproben. So ist weder die Einwilligung noch die Dokumentation auf der Karte noch die Widerruflichkeit und Beschränkung auf einzelne Anwendungen der Karte – wie sie in § 291 a Abs. 5 SGB V gefordert werden – zwingend Gegenstand der Testphase.

Zunächst aber ging es im vergangenen Jahr in Berlin um ein scheinbar banales Problem. Eine Voraussetzung der Einführung der Karte ist, dass eine einheitliche *Krankenversicherungsnummer* gebildet wird, die auch beim Wechsel der Krankenkassen konstant bleibt. Dazu darf die Rentenversicherungsnummer verwendet werden. Die gesetzliche Vorgabe ist jedoch, dass aus der Krankenversicherungsnummer weder auf die Rentenversicherungsnummer noch aus der Rentenversicherungsnummer auf die Krankenversicherungsnummer geschlossen werden kann. Zur Vergabe der Krankenversicherungsnummer auf Grundlage der Rentenversicherungsnummer wurde eine Vertrauensstelle unabhängig von den Krankenkassen geschaffen, die die Geheimhaltung der Umschlüsselungsalgorithmen wahrt.

Der Bundesgesetzgeber hat außerdem festgelegt, dass für Personen, für die noch keine Rentenversicherungsnummer vergeben wurde, diese neu zu bilden ist. Die Rentenversiche-

75 JB 2004, 4.4.2

76 VO v. 2. November 2005, BGBl. I, 3128. Rechtsgrundlage hierfür ist der durch das Gesetz zur Organisationsstruktur Telematik im Gesundheitswesen (v. 22. Juni 2005, BGBl. I, 1720) eingefügte § 291 b SGB V.

rungsnummer wird gebildet aus dem Geburtsdatum, dem Anfangsbuchstaben des Geburtsnamens und dem verschlüsselten Geschlecht. Darüber hinaus enthält der Stammdatensatz bei der Datenstelle der gesetzlichen Rentenversicherung noch Angaben zum Geburtsort einschließlich des Geburtslandes und zur Staatsangehörigkeit sowie Vor-, Zu- und Geburtsnamen und die Anschrift. Insbesondere der Geburtsort und das Geburtsland, aber auch die Staatsangehörigkeit werden dazu genutzt, Doppelt- oder Fehlvergaben von Rentenversicherungsnummern zu vermeiden. Für eine Vielzahl (bundesweit ca. 10 % der Versicherten, d. h. über sieben Millionen Personen) existiert aber keine *Rentenversicherungsnummer*, da sie entweder noch nicht oder nicht rentenversichert sind. Für die AOK Berlin – Die Gesundheitskasse waren dies 80.000 Personen. In den Daten der AOK befanden sich jedoch keine Angaben zum Geburtsnamen, Geburtsort und -land sowie auch häufig nicht zur Staatsangehörigkeit. Die fehlenden Daten waren also zu erheben.

Der Bundesgesetzgeber hat keine Regelungen getroffen, wie das zu geschehen hat; somit gelten die allgemeinen Übermittlungsregelungen des SGB X. Danach sind Sozialdaten grundsätzlich beim Betroffenen zu erheben. Weil die AOK einen erheblichen Aufwand bei der Erfassung sah, bat sie das Landesamt für Bürger- und Ordnungsangelegenheiten um eine entsprechende elektronische Ergänzung der Datensätze. Da dieses Problem in allen Bundesländern auftrat, stimmten sich die Datenschutzbeauftragen des Bundes und der Länder in ihrem Vorgehen ab. Nach eingehender Prüfung kamen auch wir zu dem Ergebnis, dass die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Versicherten beeinträchtigt werden. Dann ist die Datenerhebung bei Dritten nach einer Ausnahmeregelung im SGB X zulässig. Wir verbanden dies jedoch mit der Auflage, dass es sich dabei nur um eine einmalige Datenübermittlung handeln könne und jegliche Nutzung für andere Zwecke als für die Bildung einer Rentenversicherungsnummer unzulässig ist.

Aber auch ein weiteres Problem bei der Einführung der elektronischen Gesundheitskarte ist heute bereits sichtbar. Die elektronische Gesundheitskarte soll auf ihrer Vorderseite ein *Lichtbild* des Versicherten enthalten. Auch hier hat der Bundesgesetzgeber keine Regelungen getroffen, insbesondere nicht, ob eine explizite Pflicht der Versicherten besteht, ein Lichtbild beizubringen. Eine Krankenkasse im Norden Deutschlands wollte zu diesem Zweck, insbesondere um auch eine Erhebung bei den Betroffenen zu vermeiden, auf die Bilddaten der Personalausweisregister zurückgreifen. Im Personalausweisgesetz findet sich lediglich eine Übermittlungsregelung für konkrete Einzelfälle, so dass nach gegenwärtiger Rechtslage - von Qualität und Alter der Lichtbilder und damit der Geeignetheit dieser Bilddaten abgesehen - die Übermittlung an Krankenkassen unzulässig ist. Die AOK Berlin – Die Gesundheitskasse teilte uns mit, dass verschiedene Varianten geprüft werden. Das sind die Anforderung fertiger Bilder direkt bei den Versicherten über die

Mitgliedermagazine und/oder eine separate Mailingaktion, Aufnahmen innerhalb der AOK-Servicecenter oder mobil für besondere Personengruppen mit Personal der AOK oder auch eine Kooperation mit Fotoketten und Fachgeschäften als Datenverarbeitung im Auftrag. Es mehren sich jedoch schon Kritiken an dem geschätzten Aufwand von bundesweit ca. 250 Millionen Euro, der erforderlich ist, um die rund 60 Millionen Passfotos einzusammeln und auf die elektronische Gesundheitskarte zu übertragen.

Bei der Einführung der elektronischen Gesundheitskarte zeigt sich erneut, dass die datenschutzrechtliche Dimension mitunter nicht überblickt wird und ganze Ketten von Erhebungs- und Verarbeitungsbefugnissen nach dem Prinzip „learning by doing“ nachgebessert werden müssen. Datenschutzrechtlich gesehen sind einige Regelungen im SGB V für spätere Nutzung der elektronischen Gesundheitskarte zwar vorbildlich, für den Prozess der Vorbereitung und Einführung sind sie jedoch lückenhaft.

Bequem, aber unzulässig

Mitunter stellt sich bei der zahnärztlichen Behandlung heraus, dass der eine oder andere Zahn nur noch durch eine aufwendige Zahnersatzbehandlung gerettet werden kann. Für gesetzlich Versicherte wird in diesen Fällen nach einem bundeseinheitlichen Muster ein Heil- und Kostenplan durch den Zahnarzt erstellt, der den Befund des gesamten Gebisses enthält. Dieser Heil- und Kostenplan muss dann von der jeweiligen Krankenversicherung des Patienten bestätigt werden und die Krankenkasse erklärt dabei, in welcher Höhe sie Festzuschüsse übernimmt. Nach der Bestätigung beginnt die Behandlung und es werden beispielsweise Gebissabdrücke vorgenommen, die einem zahntechnischen Labor dazu dienen, den entsprechenden Zahnersatz zu fertigen. Der Einfachheit halber wurde mitunter dieser Heil- und Kostenplan, der Bestandteil der Abrechnung gegenüber der Krankenkasse ist und somit Sozialdaten enthält, dem zahntechnischen Labor im Rahmen der Auftragserteilung übermittelt. Die Zahntechniker-Innung Berlin-Brandenburg fragte an, ob dies zulässig ist und wenn ja, wie lange die Kopien der Heil- und Kostenpläne bei den Zahntechnikern aufzubewahren sind.

Die Aufbewahrung der Heil- und Kostenpläne als Sozialdaten bei den Krankenkassen ist zweifelsfrei zulässig. Auch die Zahnärzte haben im Rahmen der Patientenakte die Heil- und Kostenpläne als der ärztlichen Schweigepflicht unterliegende Patientendaten aufzubewahren. Die Übermittlung von Kopien der Heil- und Kostenpläne an Zahntechniker hingegen stellt einen eindeutigen Verstoß gegen die *ärztliche Schweigepflicht* dar. Dies teilten wir der Zahntechniker-Innung Berlin-Brandenburg mit, die ihre Mitglieder entsprechend darüber informierte.

Für das zahntechnische Labor ist es jedoch in keiner Weise erforderlich, die identifizierenden Daten wie Namen, Geburtsdatum, Krankenversicherungsnummer u. Ä. sowie die Höhe des bewilligten Festzuschusses und andere enthaltene Daten zur Kenntnis zu nehmen.

Die Übermittlung von Daten, die zur Erstellung medizinischer Hilfsmittel erforderlich sind und die dem Patientengeheimnis unterliegen, bedarf der ausdrücklichen Einwilligung des Patienten. Bei Heil- und Kostenplänen für Zahnersatzleistungen ist dabei nicht einmal die Erforderlichkeit gegeben.

Ein leider noch verbreitetes Problem erregte die Gemüter einiger Petenten:

> *Ein Petent erhielt ein Schreiben vom Bezirksamt Neukölln, welches sich zwar korrekt in einem verschlossenen Kuvert befand, jedoch war auf dem Kuvert sichtbar ein Stempel-Absender einer sensiblen Verwaltungseinheit (Gesundheitsamt – Sozialpsychiatrischer Dienst) für Dritte zu lesen. Ein weiterer Petent erhielt einen Brief, auf dem für Dritte deutlich lesbar eine sensible Beratungsstelle (Gesundheitsamt Steglitz, Beratungsstelle für Behinderte, Krebs- und Aidskranke) als Absender vermerkt war.*

Hierzu hatten wir die entsprechenden Ämter angeschrieben und gebeten, hinsichtlich des verwandten Stempels bzw. der Absenderangaben künftig auf derart weitgehende Bezeichnungen im Schriftverkehr mit dem Bürger zu verzichten.

Wir wiesen darauf hin, dass mit derlei Absenderangaben in die Persönlichkeitsrechte der Betroffenen eingegriffen wird. Bereits vor fast 20 Jahren[77] haben wir festgestellt, dass darauf hingewirkt werden muss, solche Zusätze entweder völlig wegzulassen oder aber die Bezeichnungen sensibler Verwaltungseinheiten so abzukürzen oder zu verschlüsseln, dass Rückschlüsse auf persönliche oder sachliche Beziehungen der Adressaten nicht möglich sind. Damit jedoch ein nicht zustellbares Schriftstück den absendenden Sachbearbeiter wieder verschlossen erreichen kann, haben wir gegen die Angabe des Stellenzeichens keine Einwände.

Die Ämter haben uns erklärt, dass bei künftigen Anschreiben an Bürger auf das Anbringen von Zusätzen, die auf sensible Verwaltungseinrichtungen hinweisen, verzichtet wird.

Probleme beim Durchsetzen der *Qualitätssicherung* im Gesundheitswesen

Im vergangenen Jahr berichteten wir über die Neukonzeption der Qualitätssicherung in der

77 JB 1986, 4.5

Nierenersatztherapie[78]. Eine Richtlinie des Gemeinsamen Bundesausschusses der Ärzte und Krankenkassen soll alle Behandlungseinrichtungen verpflichten, sich an Qualitätssicherungsmaßnahmen zu beteiligen. Diese flächendeckende Qualitätssicherung setzt jedoch voraus, dass an einer zentralen Stelle medizinische Daten aller Patienten der gesetzlichen Krankenversicherung analysiert und bewertet werden.

Nach § 135 a SGB V werden Vertragsärzte, medizinische Versorgungszentren, zugelassene Krankenhäuser, Erbringer von Vorsorgeleistungen oder Rehabilitationsmaßnahmen verpflichtet, sich an einrichtungsübergreifenden Maßnahmen zur Qualitätssicherung zu beteiligen. Allein aus dieser Verpflichtung kann jedoch nicht hergeleitet werden, dass die Patienten die Überprüfung ihrer medizinischen Daten ohne eine rechtliche Befugnis an zentrale Einrichtungen zur Qualitätssicherung dulden müssen. Die Befugnis dazu kann auch nicht von einer Einwilligung der Patienten abhängig gemacht werden, da dies einer flächendeckenden Qualitätssicherung zuwiderlaufen würde. Daher empfahl der Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zunächst zu prüfen, ob eine durchgängige Pseudonymisierung beginnend von der behandelnden Einrichtung bis zum Datenanalysten (Qualitätssicherungseinrichtung) möglich ist.

Dabei ist ein eindeutiges Merkmal erforderlich, das einerseits z. B. wiederholte Krankenhausaufenthalte derselben Person bei Rückfällen zusammenfasst, andererseits aber jedoch einen unmittelbaren Rückschluss auf den Patienten verhindert (Pseudonym). Für jede Behandlungseinrichtung muss also je nach Art der Qualitätssicherungsmaßnahme aus den gleichen Ursprungsdaten wie Name, Geburtsdatum usw. immer das gleiche Pseudonym erzeugt werden können. Dieser Algorithmus ist aber zum Schutz des Patientengeheimnisses geheim zu halten. Für die Nierenersatztherapie hieße dies, dass das Geheimnis der Patientenpseudonymisierung, sollte diese in der Behandlungseinrichtung erfolgen, über alle 1.200 derartigen Einrichtungen verteilt sein müsste. Dies stellt ein erhebliches Gefährdungspotenzial dar. Daraufhin haben wir einen Vorschlag erarbeitet, der eine zentrale Patientenliste (Namen usw., die einem dauerhaften Pseudonym zugeordnet werden) bei einem Datentreuhänder (Vertrauensstelle) vorsieht. Diese Patientenliste könnte beispielsweise aus den patientenbezogenen Abrechnungsdaten der Ärzte erstellt werden. Datenschutzrechtlich ist aber nach der gegenwärtigen Rechtslage eine Übermittlung von identifizierenden Abrechnungsdaten von den Ärzten an die Kassenärztlichen Vereinigungen für eine Pseudonymisierung rechtlich nicht zulässig. Ein solches Verfahren ist aber wegen der Verteilung der Rollen und der einzelnen Akteure und damit der beschränkten Zugriffe auf die jeweils verschlüsselten Daten zu bevorzugen. Die Verarbeitung von Patientendaten zur Qualitätssicherung ist ohne Einwilligung der Betroffenen unzulässig. Sie würde einen Verstoß gegen die *ärztliche Schweigepflicht* bedeuten. Ein Ausweg kann nur darin bestehen, dass im SGB V selbst eine

78 JB 2004, 4.4.2

Befugnisnorm geschaffen wird, die eine flächendeckende Qualitätssicherung ohne die Einwilligung des Patienten erlaubt. Kriterien bzw. Fixpunkte einer solchen gesetzlichen Vorgabe sollten sein:

- die Durchführung einrichtungsübergreifender Maßnahmen der Qualitätssicherung nur mittels pseudonymisierter Patienten- bzw. Versichertendaten,
- die Verwendung sicherer Pseudonymisierungs- und Verschlüsselungsverfahren,
- die Pseudonymisierung durch eine von Krankenkassen, Kassenärztlichen Vereinigungen oder jeweiligen Verbänden rechtlich unabhängige und von diesen räumlich, organisatorisch und personell getrennte Vertrauensstelle (Datentreuhänder),
- das Verbot einer patienten- bzw. versichertenbezogenen Zusammenführung medizinischer Daten unterschiedlicher Qualitätssicherungsverfahren und die jeweilige Trennung dieser Verfahren,
- die Übermittlungsverpflichtung des Arztes oder der Behandlungseinrichtung bezüglich der medizinischen Patientendaten.

Eine solche Befugnisnorm erlaubt es dann auch, durch Richtlinien des Gemeinsamen Bundesausschusses von Ärzten und Krankenkassen weitere Festlegungen zum Umfang, zur Struktur und zur Auswahl der medizinischen Daten, die für die Qualitätssicherung erforderlich sind, sowie zum Übermittlungsverfahren, zur Festlegung der Vertrauensstelle (Datentreuhänder) und der analysierenden Stelle zu treffen. Besonders wichtig ist aus datenschutzrechtlicher Sicht, dass die Auskunftsrechte der Betroffenen über die bei der analysierenden Stelle gespeicherten medizinischen Daten mittels der Vertrauensstelle gewährleistet werden. Da die medizinischen Daten, die zur Qualitätssicherung geliefert werden, dann nicht mehr unmittelbar der ärztlichen Schweigepflicht unterliegen und somit auch kein Beschlagnahmeschutz besteht, sollten mit der Leitung der Vertrauensstelle nur Personen beauftragt werden, die in ihrer Berufsausübung vor einer Beschlagnahme der bei ihnen gespeicherten Daten geschützt sind.

Bis die erforderliche rechtliche Befugnis geschaffen ist, können in bestimmten Regionen Pilotlösungen zur Qualitätssicherung auf Grundlage der Einwilligung der Patienten geschaffen werden. Für die Qualitätssicherung bei der Nierenersatztherapie ist dafür schon eine Reihe von Vorarbeiten erfolgt.

Organspende – aber datenschutzgerecht

Die Vivantes Netzwerk für Gesundheit GmbH fragte bei uns nach, ob es zulässig sei, Daten von Verstorbenen an die Deutsche Stiftung Organspende-Gewebe (DSO-G) für potenzielle Hornhautspenden bei Nichtvorliegen einer Einwilligungserklärung des

Verstorbenen bzw. seiner Angehörigen zu übermitteln. Dies hätte den Vorteil, dass wesentlich mehr an der Hornhaut erkrankten Patienten durch eine Transplantation geholfen werden könnte. Daher bestand die Absicht, generell die Daten potenzieller Spender zu übermitteln und erst im Nachgang die Einwilligung der nächsten Angehörigen einzuholen.

Die Zulässigkeitsvoraussetzungen für Transplantationen sind im Transplantationsgesetz als Bundesrecht geregelt. Das Transplantationsgesetz unterscheidet zwischen vermittlungspflichtigen Organen (wie beispielsweise Herz, Leber und Lunge) und nicht vermittlungspflichtigen Organen. Zu letzteren gehört auch die Hornhaut. Schon der Begriff der „nicht vermittlungspflichtigen Organe“ macht deutlich, dass eine generelle Übermittlung der Daten faktisch aller Verstorbenen an die DSO-G vom Gesetzgeber nicht gewollt war. Lediglich im Einzelfall – und zwar allein auf die vermittlungspflichtigen Organe bezogen – ist es zulässig, dass auf Verlangen des Arztes Spenderdaten vor der Einholung der Zustimmung der Angehörigen übermittelt werden dürfen. Diese Vorschrift entbindet den Arzt insoweit von seiner ärztlichen Schweigepflicht. Ziel ist es dabei, die häufig nur wenige Stunden lebensfähig aufbewahrbaren Organe schnell einem potenziellen Spendenempfänger zuzuführen. Im Unterschied dazu besteht bei Hornhaut ein solcher Zeitdruck nicht, da diese innerhalb von 72 Stunden nach dem Tod des Spenders noch transplantiert werden kann. Damit hat der Gesetzgeber ausgeschlossen, dass für die Transplantation von Augenhornhaut – im Unterschied zu den vermittlungspflichtigen Organen – eine Rechtsgrundlage für die Übermittlung der Spender- und Angehörigendaten im Einzelfall vorhanden ist.

Eine mangelnde Bereitschaft in der Bevölkerung zu Organtransplantationen kann bei nicht vermittlungspflichtigen Organen bzw. Geweben nicht durch Datenübermittlungen ausgeglichen werden, die einen Verstoß gegen die *ärztliche Schweigepflicht* darstellen.

Outsourcing im Krankenhaus

Schon seit längerer Zeit mehrten sich Anfragen, unter welchen Umständen eine Verarbeitung personenbezogener Daten im Auftrag auch außerhalb von Krankenhäusern, die dem Landeskrankenhausgesetz unterliegen, zulässig ist. Ziel war es, nicht zum unmittelbaren medizinischen Kernbereich zählende Dienstleistungen (z. B. Catering) aus den Krankenhausbetrieben auszugliedern. Dem Patientengeheimnis unterliegende Daten werden verarbeitet bei der Archivierung, bei der Wartung von Medizintechnik mit selbstständiger Datenspeicherfunktion, bei der Patientenaufnahme und ggf. bei der Kostenabrechnung, bei dem Betrieb von Rechenzentren, bei dem Betrieb einiger Telefon-

bzw. Fernsehanlagen sowie bei der Ausgliederung von Krankenhausabteilungen, in denen kaum noch medizinische, jedoch mehr pflegerische Funktionen erfüllt werden (Hotelfunktion mit medizinischer Beobachtung).

Nun ist Auftragsdatenverarbeitung im medizinischen Bereich nicht generell verboten, aber besonderen Restriktionen unterworfen, die die ärztliche Schweigepflicht absichern müssen. Es sind mittlerweile Projekte bekannt, in denen mit modernsten technischen Methoden der Kryptographie beispielsweise auch die Auftragsdatenverarbeitung durch externe Rechenzentren möglich wird. Auftragnehmer unterliegen in der Regel nicht einer beruflichen Schweigepflicht, soweit sie nicht als Arztgehilfen angesehen werden können. Der Begriff des „Arztgehilfen" – und damit des Erfüllungsgehilfen – ist aber sehr eng zu fassen. Ein arbeitsrechtliches Dienstverhältnis muss zwar nicht vorliegen; es genügt aber auch nicht, den Auftragnehmer auf das Patientengeheimnis zu verpflichten. Berufsmäßig tätige Gehilfen (beispielsweise die Krankenschwestern) müssen also in einem engen und inneren Zusammenhang mit der berufsspezifischen Tätigkeit des Arztes stehen und diesen unterstützen. Dies schließt die Einbindung des Gehilfen in die Organisation der Arztpraxis oder des Krankenhauses ein. Gehilfen sind also nicht externe Dienstleistungsunternehmen, die von außen an den Arzt herantreten und rechtlich eigenständig und selbstverantwortlich Aufträge durchführen.

Zusammenfassend konnte festgestellt werden, dass insbesondere in den Regelungen des Landeskrankenhausgesetzes von Berlin – im Unterschied zu einigen Landeskrankenhausgesetzen in anderen Bundesländern – keine Befugnisnorm für die Offenbarung von personenbezogenen Patientendaten an Dienstleistungsunternehmen enthalten ist. Lediglich eine hinreichende Pseudonymisierung der Daten würde keinen Verstoß gegen die *ärztliche Schweigepflicht*, deren Bruch nach § 203 Abs. 1 Strafgesetzbuch (StGB) unter Strafe gestellt ist, darstellen.

In diesem Zusammenhang wurde auch die Frage an uns herangetragen, ob eine hinreichende Einbindung in die Organisation des Krankenhauses dann gegeben sein kann, wenn es sich bei dem Dienstleistungsunternehmen um eine hundertprozentige Tochter des Krankenhauskonzerns handelt. Grundsätzlich unterscheidet sich diese Konstellation von der oben dargestellten nicht. Ein *Konzernprivileg*, das Übermittlungen innerhalb eines Konzerns zwischen verantwortlichen Stellen erlauben würde, wurde selbst bei der Novellierung des BDSG nicht geschaffen. Doch auch wenn man zu dem Ergebnis käme, dass die Übermittlung von Patientendaten an eine hundertprozentige Tochter des Krankenhauskonzerns bei weitgehender organisatorischer Einbindung keine Datenübermittlung darstellt, so würde dies doch von der Pflicht zur Wahrung des Patientengeheimnisses und von der ärztlichen Schweigepflicht überlagert.

Auch die Auslagerung bestimmter Teilbereiche der Verarbeitung von Patientendaten (Catering,

Pflegeabteilungen, technische Wartung) bedarf der informationellen Einwilligung der Betroffenen.

Datenschutzfreundliche Änderungen beim Neugeborenen-Screening?

> *Unmittelbar nach der Geburt kann mit Hilfe eines dem Säugling aus der Ferse entnommenen Bluttropfens, der auf eine Trockenblutkarte aufgebracht wird, untersucht werden, ob das Kind an einer seltenen, aber unbehandelt häufig zum Tod führenden Stoffwechselkrankheit leidet. Dies geschieht mit Einwilligung der Eltern, zumeist der Mutter. Alle Krankheiten, auf die hin getestet wird, sind jedoch behandelbar.*

Zur Durchführung dieses *Neugeborenen-Screening* erließ der Gemeinsame Bundesausschuss von Ärzten und Krankenkassen eine Richtlinie. Diese Richtlinie ist nicht unproblematisch, da sie sich lediglich auf 14 Zielkrankheiten beschränkt. Informationen über andere Krankheiten, die mittels des Verfahrens der „Tandemmassenspektroskopie“ festgestellt werden und auch behandelbar sind, dürfen den Eltern nicht mitgeteilt werden. In der Vergangenheit wurden die *Trockenblutkarten* faktisch unbegrenzt aufbewahrt. Die identifizierenden Merkmale wurden gesondert gelagert, so dass eine Zweckentfremdung beispielsweise für unzulässige genetische Tests auch organisatorisch erschwert wurde. Eine Beschlagnahme der Blutproben war auch in der Vergangenheit schon rechtlich ausgeschlossen. Die Richtlinie des Gemeinsamen Bundesausschusses schreibt nunmehr vor, dass die Trockenblutkarten bereits nach drei Monaten zu vernichten sind. Auch wenn eine kurze Aufbewahrungsfrist scheinbar datenschutzfreundlich und im Interesse der neugeborenen Kinder zu liegen scheint, würde den Kindern selbst und insbesondere ihren Eltern bei möglichen Fehldiagnosen (nicht erkannte Krankheiten infolge von Laborfehlern) jegliche rechtliche Möglichkeit der Überprüfung abgeschnitten.

In Berlin wird von dem in der Richtlinie vorgeschriebenen Verfahren abgewichen. Nach dem vereinbarten Vorgehen besteht die Möglichkeit, das Untersuchungsspektrum um weitere Erkrankungen im Rahmen kontrollierter Studien zu erweitern, um dadurch den Patienten die optimale Versorgung zu gewährleisten, gleichzeitig aber auch sicherzustellen, dass die Ergebnisse in eine spätere Bewertung der Parameter mit einfließen. Für das Jahr 2006 wird in diesem Rahmen ein Mukoviszidose-Screening angeboten werden. Für diese Erweiterungen wird ein separates Einverständnis eingeholt. Die Aufbewahrung der Restblutproben ist in Berlin bis zur Volljährigkeit des Patienten festgelegt. Dazu werden die Restblutproben nach einem Jahr pseudonymisiert und alle persönlichen Daten werden einem Treuhänder übergeben. Eine spätere Zuordnung der Restblutproben zu den persönlichen Daten ist nur auf Antrag der Eltern möglich. Die ausdrückliche schriftliche und informierte Einwilligung der Eltern in dieses Verfahren vorausgesetzt, halten wir das Abweichen von der Richtlinie des Gemeinsamen Bundesausschusses nicht nur für zulässig, sondern vor allem auch im Interesse der Kinder und deren Eltern liegend.

Seit nunmehr einigen Jahren entwickelt sich ein zweites Neugeborenen-Screening flächendeckend in Berlin. Unterstützt durch Spenden eines Berliner Lions-Clubs wurden, ohne dass dies eine Leistung der gesetzlichen Krankenversicherung ist, Geräte angeschafft, mit denen unmittelbar nach der Geburt Signale gemessen werden können, die fundierte Hinweise auf Taubheit oder Schwerhörigkeit geben. Initiiert wurde dies vom *Deutschen Zentralregister für kindliche Hörstörungen*, das unter dem Dach der Charité mit Einwilligung der Erziehungsberechtigten seit 10 Jahren tätig ist und Grundlage für eine Reihe von Forschungsprojekten bildet. Da somit in den ersten Tagen nach der Geburt insbesondere der Mutter zwei verschiedene Aufklärungsschriften und Einwilligungserklärungen vorgelegt werden sollten, empfahlen wir, beide Screening-Maßnahmen miteinander zu verbinden. Daraufhin wurde eine gemeinsame Aufklärungs- und Informationsbroschüre entwickelt und die entsprechenden Materialien werden inzwischen in mehr als drei Bundesländern erfolgreich eingesetzt. Ein Erfolg dieses Screenings bei vermuteter Hörstörung setzt voraus, dass in den nach der Geburt folgenden Monaten das Kind noch weiteren Untersuchungen unterzogen werden muss. Mit Einwilligung der Eltern stellt das Deutsche Zentralregister für angeborene Hörstörungen sicher, dass auf Grundlage der erhobenen Adressdaten die Eltern kontaktiert werden, die erforderlichen Untersuchungen durchzuführen. Seit Einführung des Hörscreenings konnten somit 15 Kinder mit Hörstörungen identifiziert und nachfolgend behandelt werden. In der Vergangenheit wurden Hörstörungen zumeist erst zwischen dem zweiten und dem sechsten Lebensjahr festgestellt, so dass die Kinder einen nicht wieder aufholbaren Entwicklungsrückstand insbesondere bei der Sprachentwicklung gegenüber Gleichaltrigen hatten.

Wir haben Verbesserungen bei der Speicherung von Ergebnissen des Neugeborenen-Screenings und eine Verknüpfung paralleler Initiativen in diesem Bereich erreicht.

Mammographie-Screening – nun doch mit Meldedaten

Unter der Überschrift „Meldedaten für Mammographie-Screening“ berichteten wir im Jahresbericht 2004[79] über die rechtlichen Probleme bei der Durchsetzung des von dem Bundesausschuss der Ärzte und Krankenkassen im Rahmen der *Krebsfrüherkennungs-Richtlinie* beschlossenen Mammographie-Screenings für alle Frauen ab dem Alter von 50 Jahren bis zum Ende des 70. Lebensjahres. Die regelmäßige Übermittlung von Meldedaten, um die Einladungen aller – und nicht nur der gesetzlich krankenversicherten – Frauen durchführen zu können, bedurfte melderechtlich zweierlei Voraussetzungen:

Die die Frauen einladende „zentrale Stelle“ musste datenschutzrechtlich eine öffentliche Stelle sein. Nur unter dieser Bedingung ist es rechtlich zulässig, dass die Meldedaten wie Name, Adresse,

79 vgl. 4.4.2

Geburtsname sowie Ort und Tag der Geburt nach § 26 Abs. 2 Berliner Meldegesetz (MeldeGBln) von der Meldebehörde an die einladende „zentrale Stelle“ übermittelt werden. Zunächst erscheint es jedoch nicht einleuchtend, dass für die Einladung der Frauen neben Namen und Adressen auch der Geburtsname sowie Tag und Ort der Geburt der einladenden „zentralen Stelle“ zur Verfügung gestellt werden. Der Datenbezug beschränkt sich auf den in den Krebsfrüherkennungs-Richtlinien festgelegten Umfang. Dieser Umfang ergibt sich aus der Notwendigkeit, den von der Zentralen Stelle einzuladenden Frauen bereits zum Zeitpunkt der Einladung eine eindeutige, lebenslang geltende Screening-Identifikationsnummer zuzuordnen, da die personenbezogenen Daten nach erfolgter Einladung und ggf. Erinnerung gelöscht werden und für die Erkennung zur turnusmäßigen Wiedereinladung nicht mehr zur Verfügung stehen. Die Identifikationsnummern sind nach einem bundesweit einheitlichen Algorithmus aus dem ersten Vornamen, Geburtsnamen, Geburtsdatum und Geburtsort zu bilden. Unter frühere Namen fällt auch der Geburtsname. Würden weniger als diese vier Angaben zur Bildung der Identifikationsnummern verwendet, bestünde die Gefahr der Mehrdeutigkeit. Andere Angaben, z. B. Familiennamen, können dagegen die lebenslange Gültigkeit verlieren.

Die personenbezogenen Melderegisterdaten werden außerdem zur Bildung einer Kontrollnummer nach dem vom Gemeinsamen Krebsregister verwendeten Algorithmus herangezogen, damit ein regelmäßiger anonymisierter Abgleich mit den Daten des *Krebsregisters* stattfinden kann. Der Abgleich dient der Feststellung falschnegativer Diagnosen bzw. von Intervallkarzinomen bei den Frauen, die am Screening teilgenommen haben, und schafft damit auch die Voraussetzung dafür, dass die Zentrale Stelle die inzwischen an Brustkrebs erkrankten Frauen nicht zu Widerholungsuntersuchungen einlädt.

Des Weiteren soll durch eine unabhängige Stelle untersucht werden, mit welcher Qualität das Mammographie-Screening durchgeführt wurde. Erkrankt beispielsweise im Intervall zwischen zwei Untersuchungen eine Frau an Brustkrebs, so soll durch eine externe Begutachtung der von der untersuchenden Einrichtung (*Screening-Einheit*) gefertigten Aufnahmen der letzten Untersuchung die Qualität der Diagnose überprüft werden. Auch dazu ist die Nutzung eines eindeutigen Identifikators erforderlich. Der Identifikator wird unter Nutzung von Geburtsnamen, Tag und Ort der Geburt bei der „zentralen Stelle“ gebildet. Die „zentrale Stelle“ hält jedoch diese Daten danach nicht mehr vor, sondern löscht sie. Damit wird einer datenschutzrechtlichen Forderung Rechnung getragen. Die Software zur Bildung des Identifikators für den Abgleich mit dem Krebsregister ist die gleiche, die durch das Gemeinsame Krebsregister genutzt wird. Sie stellt ein Geheimnis dar, das in der Vertrauensstelle des Krebsregisters gewahrt wird. Die Übermittlung dieses Geheimnisses an die „zentrale Stelle“ zur Bildung des Identifikators bedurfte ebenfalls einer rechtlichen Befugnis. Somit musste der Staatsvertrag über das Gemeinsame Krebsregister dahingehend geändert werden. Die Änderungen zum Staatsvertrag sind im November dem Abgeordnetenhaus von Berlin zur

Kenntnisnahme vorgelegt wurden; der Entwurf für ein Gesetz zur Berechtigung der „zentralen Stelle“ als öffentliche Stelle und zur Übermittlung von Meldedaten an diese wurde Ende 2005 auf Referentenebene fertig gestellt.

Mit erheblicher zeitlicher Verzögerung wird jetzt entsprechend unserem schon früh gemachten Vorschlag die Nutzung von Meldedaten für die Einladung zum Mammographie-Screening ermöglicht.

Presseveröffentlichung in einem Sozialgerichtsprozess

Das Sozialgericht hat im Rahmen eines „Medizin-Regressprozesses“ eine Entscheidung getroffen zu der Frage, ob eine Krankenkasse für ein verordnetes Medikament aufkommen muss, das für die spezielle Anwendung nicht zugelassen war, aber die einzige Möglichkeit bot, einem schwer kranken Patienten zu helfen. Der Pressesprecher des Sozialgerichts wollte von uns wissen, ob in der Pressemitteilung und dem Urteil, das veröffentlicht werden soll, der unterlegene Arzt als solcher benannt werden darf, welche persönlichen Angaben über ihn zulässig sind und ob zumindest die Klinik, der der Arzt angehört, auf Nachfrage Dritter genannt werden darf. Darüber hinaus stellte sich für künftige Fälle die Frage, ob der Hinweis auf eine bevorstehende Gerichtsverhandlung anders zu bewerten ist als ein nachträglicher Bericht über den Inhalt der Entscheidung und ob es einen Unterschied macht, dass eine öffentliche Verhandlung oder nur ein schriftliches Verfahren stattgefunden hat.

Nach § 6 Abs. 1 Satz 2 BlnDSG ist die Verarbeitung personenbezogener Daten nach diesem Gesetz zulässig, wenn wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Bei dem betroffenen Arzt handelte es sich um eine „bekannte Größe“ im medizinischen Bereich. Zudem ging es bei dem Prozessgegenstand um eine Angelegenheit von hohem öffentlichen Interesse. Deshalb war davon auszugehen, dass schutzwürdige Belange des Arztes durch die Bekanntgabe seiner Funktionsbezeichnung in der Pressemitteilung und im Urteil nicht beeinträchtigt werden. Eine solche Beeinträchtigung kann aber vorliegen, wenn es im Prozess um ein „ehrenrühriges“ vorwerfbares Verhalten geht (z. B. im Betrugsfall). Schutzwürdige Belange können darüber hinaus sowohl beim Hinweis auf eine bevorstehende Gerichtsverhandlung als auch bei einem nachträglichen Bericht über den Inhalt einer Entscheidung beeinträchtigt sein. Im ersten Fall ist dies nur dann zu verneinen und die Veröffentlichung zulässig, wenn es sich ausschließlich um die Terminankündigung und eine sparsame Beschreibung des Prozessgegenstandes handelt. Dies gilt wiederum nur für die Information durch Aushang im Gericht und der örtlichen Presse (Print–Medien, Rundfunk und Fernsehen). Eine Verbreitung über das weltweite Medium des Internet wäre nicht zulässig. Die Öffentlichkeit mündlicher Verhandlungen allein führt nicht zur Zulässigkeit der Datenverarbeitung. Stets muss geprüft werden, ob schutzwürdige Belange der Betroffenen durch die Veröffentlichung der Daten beeinträchtigt werden. Eine Offenbarung des Namens des Arztes und der Funktionsbezeichnung auf Anfrage Dritter war nach § 6 Abs. 1 i. V. m. Abs. 2 Satz 1 Nr. 1 a) IFG zulässig. Nach § 2 Abs. 1 letzter Satz IFG gilt das Gesetz für die Gerichte nur, soweit sie Verwaltungsaufgaben erledigen. Hierzu gehört die Veröffentlichung der gerichtlichen Entscheidung und der Pressemitteilung, denn dies stellt keine „echte“ Tätigkeit der Judikative dar.

Es muss stets im Einzelfall geprüft werden, ob die Veröffentlichung von personenbezogenen Daten von Prozessbeteiligten durch das Gericht zulässig ist. Maßgeblich ist, dass schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

4.5.2 Sozial- und Jugendverwaltung

Anforderung medizinischer Unterlagen durch Sachbearbeiter des Sozialamtes

> *Mehrere Bürger wandten sich an uns und schilderten, sie seien im Verfahren zur Feststellung der dauerhaften vollen Erwerbsminderung von der Abteilung Soziales eines Bezirksamtes aufgefordert worden, ein Erklärungsformular über die Entbindung von der ärztlichen Schweigepflicht zu unterschreiben. Diese Erklärung sollte es den Sozialleistungs- und Rentenversicherungsträgern erlauben, von den behandelnden Ärzten und Einrichtungen ärztliche und psychologische Untersuchungsunterlagen anzufordern. Die Betroffenen waren verunsichert und fragten uns, ob die Mitarbeiter des Sozialamtes, die gerade nicht zum medizinischen Personal gehören, befugt sind, sensible ärztliche Unterlagen anzufordern.*

Hintergrund der Anforderung der Schweigepflichtentbindungserklärungen war ein Verfahren zur Prüfung, ob Leistungen der *Grundsicherung* bei Erwerbsminderung zu gewähren waren. Voraussetzung für den Anspruch ist die Feststellung des Vorliegens einer dauerhaften vollen Erwerbsminderung.

Leistungen der Grundsicherung wurden bis zum 31. Dezember 2004 von den Grundsicherungsträgern nach den Vorschriften des Grundsicherungsgesetzes (GSiG) gewährt. Mit der Eingliederung der Sozialhilfe in das neu geschaffene Sozialgesetzbuch – Zwölftes Buch (SGB XII) wurde das bisherige Bundessozialhilfegesetz ersetzt. Gleichzeitig wurde das GSiG aufgehoben und die Vorschriften über die Gewährung von Leistungen der Grundsicherung im Alter und bei Erwerbsminderung wurden in das neue SGB XII aufgenommen. Träger der Leistungen der Grundsicherung sind nunmehr die Träger der Sozialhilfe.

Nach der alten Rechtslage nach dem GSiG war es unklar, ob der Grundsicherungsträger befugt war, selbst über das Vorliegen einer Erwerbsminderung zu entscheiden oder ob er die medizinische Entscheidung darüber allein dem Rentenversicherungsträger als fachlich geeigneter Stelle überlassen musste und an diese Entscheidung gebunden war. In der Vergangenheit hatte dies zur Folge, dass teilweise umfangreiche Schweigepflichtentbindungserklärungen von den Betroffenen angefordert wurden. Diese Verfahrensweise haben wir wiederholt kritisiert.

Durch den neuen § 45 SGB XII ist nunmehr klargestellt, dass der Träger der Sozialhilfe den zuständigen Träger der Rentenversicherung ersucht, die medizinischen Voraussetzungen einer dauerhaften vollen Erwerbsminderung zu prüfen, wenn es „aufgrund der Angaben und Nachweise des Leistungsberechtigten als wahrscheinlich erscheint, dass diese erfüllt sind und das zu berücksichtigende Einkommen und Vermögen nicht ausreicht, um den Lebensunterhalt vollständig zu decken. Die Entscheidung des Trägers der Rentenversicherung ist für den ersuchenden Träger der Sozialhilfe bindend."

Damit ist klargestellt, dass die medizinische Begutachtung ausschließlich den Rentenversicherungsträgern obliegt. Eine Anforderung weiterer Unterlagen bei Ärzten oder Einrichtungen ist dagegen nicht erforderlich. Der Träger der Sozialhilfe ist auch nicht befugt, eine Erklärung über die Entbindung von der ärztlichen Schweigepflicht einzuholen, die es ihm erlaubt, ärztliche Untersuchungsunterlagen über den Betroffenen bei Dritten anzufordern. Für die Feststellung der Wahrscheinlichkeit einer dauerhaften vollen Erwerbsminderung durch den Träger der Sozialhilfe ist es ebenfalls nicht erforderlich, Unterlagen von Dritten zu beschaffen. Vielmehr stellt § 45 Abs. 1 Satz 1 SGB XII klar, dass es auf die „Angaben und Nachweise des Leistungsberechtigten" ankommt.

Im konkreten Einzelfall hat das Bezirksamt den verwendeten Vordruck nach unseren Vorgaben überarbeitet. Die von den Betroffenen angeforderte Erklärung über die Entbindung von der Schweigepflicht erlaubt es nunmehr ausschließlich den Rentenversicherungsträgern, weitere Unterlagen von den im Antrag angegebenen Ärzten und Einrichtungen anzufordern. Außerdem werden die Betroffenen darauf hingewiesen, dass die von ihnen eingereichten Gutachten und Atteste über die als Ursache für die Erwerbsminderung im Antrag angegebene Behinderung oder Krankheit ausschließlich an den Rentenversicherungsträger weitergegeben werden.

Da die ursprünglich verwendeten Vordrucke für die Erklärung der Entbindung von der ärztlichen Schweigepflicht nicht von dem einzelnen Bezirksamt entwickelt, sondern offenbar von den Rentenversicherungsträgern zur Verfügung gestellt worden waren, halten wir eine Überarbeitung dieser Erklärungen sowie des Verfahrens zur Feststellung der dauerhaften vollen Erwerbsminderung für erforderlich, um auf diese Weise berlinweit eine einheitliche Verfahrensweise erreichen zu können. Aus diesem Grund sind wir mit unserem Anliegen an die zuständige Senatsverwaltung herangetreten. Von dort wurde uns die Bereitschaft signalisiert, eine Überarbeitung der Vordrucke vorzunehmen.

Durch die an uns herangetragenen Beschwerden konnte erreicht werden, dass das Verfahren zur Feststellung der dauerhaften vollen

Erwerbsminderung in dem Bezirksamt datenschutzgerechter gestaltet werden konnte. Wir sind bestrebt, im Interesse der Betroffenen ein berlinweit einheitliches datenschutzkonformes Verfahren zu entwickeln.

Unberechtigte Weitergabe von Daten durch das Sozialamt an den Vermieter

Der Berliner Mieterverein wandte sich für ein Mitglied an uns und beschwerte sich darüber, dass ein Sozialamt einem Vermieter auf dessen Anforderung hin die Höhe der an das Mitglied monatlich gezahlten Miete schriftlich mitgeteilt hat. Der Sachverhalt wurde von dem entsprechenden Sozialamt als zutreffend bestätigt.

Die Datenübermittlung durch das Sozialamt war rechtswidrig. Es handelte sich bei den Angaben über den Leistungsbezug um Sozialdaten, für deren Übermittlung eine gesetzliche Befugnis nach den §§ 68 bis 77 Sozialgesetzbuch – Zehntes Buch (SGB X) oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegen muss. Dieses war jedoch nicht der Fall. Auch eine ausdrückliche Einwilligung des betroffenen Mitglieds in die Datenübermittlung lag nicht vor.

Wir haben dem Bezirksamt unsere Rechtsauffassung hinsichtlich der Unzulässigkeit der Datenübermittlung mitgeteilt. Gleichzeitig haben wir den Fall zum Anlass genommen, das Sozialamt aufzufordern, generelle Maßnahmen zu treffen, um zu verhindern, dass sich ähnliche Vorfälle in Zukunft wiederholen können. Das Sozialamt ist unserer Forderung nachgekommen und hat die Mitarbeiterinnen und Mitarbeiter entsprechend angewiesen.

Eine Übermittlung von Sozialdaten kann nur dann zulässig sein, wenn hierfür eine Übermittlungsbefugnis nach dem Sozialgesetzbuch, insbesondere den Vorschriften des SGB X, besteht oder aber eine wirksame Einwilligung des Betroffenen vorliegt. Auch in Fällen, in denen der Dritte, an den die Sozialdaten übermittelt werden sollen, Kenntnis von dem Leistungsbezug hat, ist eine Übermittlung der Leistungshöhe durch den Sozialleistungsträger ohne Rechtsgrundlage oder eine wirksame Einwilligung des Betroffenen keinesfalls zulässig.

Neue Rechtsgrundlagen für die Kindertagesbetreuung

Mit dem zum 1. August 2005 in Kraft getretenen

Kindertagesbetreuungsreformgesetz[80] werden die Rechtsgrundlagen über die *Kindertagesbetreuung* grundlegend novelliert. Damit werden rechtliche Grundlagen für die Umsetzung bestimmter Reformvorhaben in diesem Bereich (z. B. Umstrukturierung der Hortbetreuung, Übertragung der Verantwortung für die Finanzierung der Kindertagesbetreuung auf die Bezirke, sog. Gutscheinfinanzierung) geschaffen.

Aus datenschutzrechtlicher Sicht ist es erfreulich, dass mit der Schaffung des neuen Gesetzes auch die Rechtsvorschriften über die Kostenbeteiligungspflicht novelliert worden sind. Bislang war für die Ermittlung und Einziehung der Kostenbeteiligung der Träger der Einrichtung zuständig. Diese Rechtslage hat in der Vergangenheit Anlass zu Beschwerden betroffener Eltern bei uns gegeben, weil sie den Trägern gegenüber ihre Einkommenssituation offen legen mussten und dagegen datenschutzrechtliche Bedenken hatten. Da nach bisheriger Rechtslage die Zuständigkeit für die Ermittlung und Einziehung der Beiträge durch die Träger gesetzlich geregelt war, mussten wir den Betroffenen mitteilen, dass die Datenerhebung rechtlich zulässig ist. Da die Berechnung der Kostenbeteiligung nunmehr mit der Bedarfsfeststellung durch das zuständige Jugendamt verbunden ist, setzt das Jugendamt auch die Kostenbeteiligung durch Bescheid fest, ohne dass die Träger in das Verfahren involviert sind.

Aus unserer Sicht kann mit dieser neuen Rechtslage den Interessen der betroffenen Eltern Genüge getan werden, da sie die Angaben über das für die Kostenbeteiligung erforderliche Einkommen nicht mehr den Trägern der Einrichtung, sondern ausschließlich dem Jugendamt, das strengeren Datenschutzvorschriften unterliegt, mitteilen müssen.

4.5.3 Personaldatenschutz

***Rosenholz-Dateien* lösen neue Überprüfungswelle aus**

Ein Petent war seit 1992 Beschäftigter eines Bezirksamts. Er beschwerte sich über ein Schreiben des Personalamts, in dem er aufgefordert wurde, sein Einverständnis zu erteilen, sich von der Beauftragten für die Stasi-Unterlagen überprüfen zu lassen. Er teilte mit, seit Februar 2002 nicht mehr im Dienst zu sein, weil er arbeitsunfähig sei. Eine Rückkehr an den alten Arbeitsplatz sei sehr unwahrscheinlich.

Der Bundesrat hatte im Jahr 2003 eine Entschließung verabschiedet,

80 Gesetz zur Weiterentwicklung des bedarfsgerechten Angebotes und der Qualität von Tagesbetreuung (Kindertagesbetreuungsreformgesetz) v. 23. Juni 2005, GVBl., 322

wonach Bund und Länder die mit der Freigabe der Rosenholz-Dateien gewonnenen neuen Erkenntnisse nutzen sollen, um weiteren Aufschluss über eine mögliche Tätigkeit von Bediensteten für den Staatssicherheitsdienst der ehemaligen DDR zu erhalten.

Besondere Rechtsvorschriften oder neue Richtlinien der Senatsverwaltung für Inneres nach dem Fund und Übergabe der Rosenholz-Dateien gibt es nach telefonischer Rücksprache mit der Senatsverwaltung nicht. Insoweit gelten für die Durchführung der Überprüfung die „Ausführungsvorschriften zur Überprüfung auf MfS-Mitarbeit“ vom 12. März 1993.

Wie bereits in unserem Jahresbericht von 1993[81] ausgeführt, bestehen für die Überprüfung so genannter Westbediensteter keine Rechtsgrundlagen; ihre Überprüfung ohne entsprechendes Einverständnis wäre daher rechtswidrig.

Im Übrigen hat eine Überprüfung grundsätzlich dann zu unterbleiben, wenn eine Kündigung des Beschäftigten oder die Nichtberücksichtigung eines Bewerbers unabhängig vom jeweiligen Überprüfungsergebnis aufgrund besonderer Umstände von vornherein auszuschließen ist .

Dagegen können und sollten weiterhin Überprüfungen durchgeführt werden, wenn der konkrete Verdacht besteht, dass ein Sachverhalt vorliegt, der personelle Maßnahmen rechtfertigen würde.

Im vorliegenden Fall war der Petent seit 2002 krankheitsbedingt nicht mehr im Dienst, eine Rückkehr an den alten Arbeitsplatz galt als unwahrscheinlich. Auch blieb sein nach der Wiedervereinigung begonnenes Arbeitsverhältnis offensichtlich jahrelang unbeanstandet, so dass eine Kündigung nach der Rechtsprechung keinen Erfolg hätte.

Schließlich ist darauf hinzuweisen, dass Unterlagen des Staatssicherheitsdienstes nach dem 30. Dezember 2006 nicht mehr zur

81 vgl. 4.5.5

Überprüfung von öffentlichen Bediensteten verwendet und diesen eine Tätigkeit für den Staatssicherheitsdienst dann nicht mehr vorgehalten oder zu ihren Nachteilen verwendet werden darf (§§ 20 Abs. 3, 21 Abs. 3 StUG).

Im Ergebnis ist festzustellen, dass die erneute generelle Überprüfung nur im Rahmen der genannten Voraussetzungen und jedenfalls nur mit dem Einverständnis der Beschäftigten erfolgen darf. Die Überprüfung sollte in den Fällen unterbleiben, in denen sie nicht zu arbeitsrechtlichen Konsequenzen führen kann.

Beantragung von technischen Hilfsmitteln bei Behinderungen

Ein Beschäftigter des Landes Berlin teilte mit, aufgrund seiner krankheitsbedingten Behinderung bei seiner zuständigen Personalstelle der Senatsverwaltung für Wirtschaft, Arbeit und Frauen ein technisches Hilfsmittel am Arbeitsplatz beantragt zu haben. Dieser Antrag sei zum Zwecke der Finanzierung an das Landesamt für Gesundheit und Soziales – Integrationsamt – weitergeleitet worden. Auf Nachfrage des Integrationsamtes, ob die Notwendigkeit des beantragten Hilfsmittels durch ein medizinisches Gutachten nachgewiesen sei, habe seine Personalstelle mitgeteilt, dass eine amtsärztliche Untersuchung hinsichtlich einer dauernden Dienstunfähigkeit des Petenten veranlasst worden sei.

Das Personalamt bestätigte uns gegenüber diesen Sachverhalt und begründete die Vorgehens-weise mit dem Hinweis, das Ergebnis einer amtsärztlichen Untersuchung würde dem Integrationsamt für die Beurteilung der medizinischen Erforderlichkeit des vom Petenten beantragten Hilfsmittels wichtige Rückschlüsse ermöglichen. Insoweit sei es notwendig gewesen, das Integrationsamt über den dem Antrag zugrunde liegenden Sachverhalt umfassend zu unterrichten, insbesondere soweit medizinische oder behinderungsbezogene Umstände berührt waren.

Bei der Tatsache, dass bei dem Beschäftigten eine amtsärztliche Untersuchung zur Feststellung seiner dauernden Dienstunfähigkeit von der Personalstelle veranlasst wurde, handelt es sich um ein Personalaktendatum. Die Zulässigkeit seiner Verarbeitung oder Nutzung richtet sich nach den Vorschriften des § 56 ff. Landesbeamtengesetz (LBG). Nach § 56 d Abs. 2 LBG dürfen Auskünfte an Dritte nur mit Einwilligung des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. Nach § 80

Abs. 5 Sozialgesetzbuch IX (SGB IX) haben die Arbeitgeber dem Integrationsamt auf Verlangen die Auskünfte zu erteilen, die zur Durchführung der besonderen Regelungen zur Teilhabe Schwerbehinderter und ihnen gleichgestellter behinderter Menschen am Arbeitsleben notwendig sind.

Im vorliegenden Fall hatte das Integrationsamt lediglich beim Personalamt nachgefragt, ob die Notwendigkeit des beantragten Gerätes durch ein medizinisches Gutachten nachgewiesen sei. Insoweit hätte die Auskunft des Personalamts ausgereicht, dass eine amtsärztliche Untersuchung eingeleitet worden ist. Keinesfalls bedurfte es dagegen des zusätzlichen Hinweises, dass diese zur Klärung der Frage, ob eine dauernde Dienstunfähigkeit vorliegt, veranlasst wurde.

Die Übermittlung dieser *Überschussinformation* durch das Personalamt verstieß gegen geltendes Personalaktenrecht und war damit unzulässig. Der Leiter des Personalamtes wurde entsprechend unterrichtet.

Teilnahme von betriebsfremden Personen an „Krankenrückkehrgesprächen“

Um einem hohen Krankenstand entgegenzuwirken, plante ein bekanntes Gesundheits-unternehmen so genannte „Fehlzeitengespräche“ bzw. „Krankenrückkehrgespräche“ mit Beschäftigten, die über einen längeren Zeitraum erhöhte krankheitsbedingte Fehlzeiten aufwiesen, zu führen. Diese sind seit Mai 2004 bundesrechtlich im Rahmen des „betrieb-lichen Eingliederungsmanagements“ vorgeschrieben und zugleich notwendige Voraussetzung für eine spätere krankheitsbedingte Kündigung (§ 84 Abs. 2 SBG IX). In den Gesprächen sollten auch persönliche Probleme sowie Diagnosen zur Sprache kommen. Zu diesen Gesprächen luden Abteilungsleiter Fachvorgesetzte ein, die keine Beschäftigten des Unternehmens waren. Die Beschäftigten selbst wünschten die Teilnahme der Fachvorgesetzten der Tochtergesellschaften an diesen Gesprächen nicht und teilten dies auch immer wieder den zuständigen Abteilungsleitern mit.

Nach höchstrichterlicher Rechtsprechung sind die Erhebung von Gesundheitsdaten ebenso wie allgemeine Fragen nach dem Gesundheitszustand nur insoweit zulässig, als gezielt Beeinträchtigungen der Verwendung auf dem vorgesehenen Arbeitsplatz ermittelt werden sollen. Folgende Fragestellungen wurden dem gemäß als zulässig erachtet:

1. Liegt eine Krankheit bzw. Beeinträchtigung des Gesundheitszustandes vor, durch die die

Eignung für die vorgesehene Tätigkeit auf Dauer oder wiederkehrend eingeschränkt ist?

2. Liegen ansteckende Krankheiten vor, die Kollegen oder Kunden gefährden könnten?

3. Ist in absehbarer Zeit mit längerer Arbeitsunfähigkeit zu rechnen, z. B. durch Operation, Kur oder akute schwer wiegende Erkrankung?

Eine darüber hinausgehende Offenbarungspflicht der Beschäftigten besteht bei Anlegung dieser von den Gerichten entwickelten Maßstäbe auch im Rahmen so genannter „Krankenrückkehrgespräche“ nicht.

Gesundheitsdaten genießen wegen ihrer hohen Sensitivität ähnlich wie Personalaktendaten einen hohen Schutz und dürfen nur im unbedingt erforderlichen Umfang erhoben und verarbeitet werden. Krankenrückkehrgespräche sollten aus diesem Grunde nur zwischen Mitarbeitern der Personalstelle und dem Beschäftigten und, wenn dieser es wünscht, in Anwesenheit eines Betriebsratsmitgliedes geführt werden. Keinesfalls erscheint es erforderlich, den jeweiligen Fachvorgesetzten zu solchen Gesprächen hinzuzuziehen.

Krankenrückkehrgespräche unterliegen darüber hinaus dem Mitbestimmungsrecht des Betriebsrats und können auch Gegenstand von Betriebsvereinbarungen sein. Die dokumentierten Ergebnisse solcher Gespräche dürfen nur den daran beteiligten Personen zugänglich gemacht werden.

Die Teilnahme von Fachvorgesetzten an Krankenrückkehrgesprächen ist ohne ausdrückliche Zustimmung des Betroffenen unzulässig.

4.5.4 Wohnen

Wohnungsbewerber und Datenschutz

> *Wohnungssuchende Petenten schickten uns immer aufs Neue Fragebögen von Hausverwaltungen und Maklern, auf denen sie nach ihrem Beruf, dem Arbeitgeber, dem Beschäftigungszeitraum bei diesem Arbeitgeber, nach dem Beruf des Ehegatten, nach der Anschrift des Arbeitgebers, dessen Telefonverbindung, dem Nettoeinkommen, nach Rentenbezug, Sozialhilfebezug, nach Angaben zur derzeitigen Wohnung (ob Altbau oder Neubau oder sozialer Wohnungsbau), nach Dauer des derzeitigen Mietverhältnisses, Zimmerzahl, Quadratmeterzahl, monatlicher Miete, Namen und*

Anschrift des bisherigen Hausverwalters, Kündigungsgrund des Vermieters, nach überfälligen sonstigen privaten oder geschäftlichen Verpflichtungen, nach der Nationalität, der ethnischen Zugehörigkeit und Staatsangehörigkeit gefragt wurden. Ferner sollte der Wohnungssuchende unterschreiben: „Mit der Auskunftseinholung über mich/uns durch den Vermieter bin ich/sind wir einverstanden und ...“

Der Datenschutz beim Abschluss von Mietverträgen beschäftigte uns im Berichtsjahr besonders intensiv. Zwar hatten wir uns bereits im Jahresbericht 1996[82] dieses Themas angenommen, jedoch war im vergangenen Jahr festzustellen, dass die Neugier von Vermietern auf die private Lebenssituation potenzieller Mieter ebenso gewachsen ist wie der Ärger von Wohnungssuchenden darüber, dass bei Wohnungsbewerbungen von Vermietern häufig private Daten erfragt werden, die in keinerlei Zusammenhang mit dem Zweck des angestrebten Mietvertrages zu bringen sind.

Wir mussten feststellen, dass nicht nur unangemessene Mengen von Daten erfragt wurden, mittels breit angelegter Fragebögen, sondern auch dass die erfragten Daten für eine Bewerberauswahl überwiegend ungeeignet waren. Auch in unserem Bericht von 1999 hatten wir darauf hingewiesen, dass Daten zur Nationalität, zur Volksgruppenzugehörigkeit, zum Beruf, zur Religion, zu den Motiven des Wohnungswechsels, Ausweisdaten (Personalausweisnummer, Passnummer), Beruf und Arbeitgeber für den Abschluss eines Mietvertrages nicht erforderlich und ihre Erhebung deshalb unzulässig ist. Nachdem 1993 der Verband Berlin-Brandenburgischer *Wohnungsunternehmen* unserer rechtlichen Bewertung zugestimmt hatte, haben wir uns nun an weitere Verbände gewandt, um auf eine Verbesserung der Situation hinzuwirken. Denn dem einzelnen Hauseigentümer ist die Nichterforderlichkeit seiner Datenneugierde nur schwer vermittelbar, wenn rundum Makler und Hausverwalter die Anfrage großer Mengen ungeeigneter Daten über die persönliche Lebenssituation von Wohnungsinteressenten empfehlen. In der Rechtsprechung wurde wiederholt und unmissverständlich deutlich gemacht, dass im Rahmen des § 28 Abs. 1 Nr. 1 BDSG bei Mietverträgen nur solche Daten bei der Bewerberauswahl oder zum Vertragsschluss abgefragt werden dürfen, die eine Relevanz für das geplante Vertragsverhältnis aufweisen. Vermieter haben nicht das Recht, die Daten ihrer Wohnungsbewerber losgelöst vom Zweck des Vertragsverhältnisses zu verarbeiten. In Zeiten einer nachlassenden Wohnungsknappheit hat diese Unsitte leider gleichwohl eher zu- als abgenommen. Hier wird das informationelle Selbstbestimmungsrecht der Bürger unmittelbar und spürbar beeinträchtigt.

Wir machten darauf aufmerksam, dass unzulässige Fragen auch nicht wahrheitsgemäß beantwortet werden müssen, so dass durch sie keine Erkenntnisse gewonnen werden können.

---

82 vgl. 3.3

Besser ist es folglich, derartige Fragen gar nicht erst zu stellen.

Es wäre zu wünschen, dass Vermieter keine unzulässigen Daten erheben und Wohnungsinteressenten auf ein solches Ansinnen sich nicht einlassen; denn das Datenschutzrecht steht auf ihrer Seite.

Vermieter, Makler und Hausverwalter müssen sich bei der Erhebung von Daten bei Wohnungsbewerbern darauf beschränken, was für den Abschluss eines Mietvertrages geeignet und erforderlich ist. In der Praxis wird dies noch zu wenig beachtet.

4.6 Wissen und Bildung

4.6.1 Wissenschaft und Forschung

Neuordnung der Studentendaten

Im vergangenen Jahr[83] berichteten wir über die Neufassung der Datenschutzregelung im Berliner Hochschulgesetz. Das Berliner Hochschulgesetz folgt zunächst der Systematik, nach der die Grundsätze der Verarbeitung personenbezogener Daten im Gesetz zu regeln sind. Zugleich wird den Hochschulen eingeräumt, mittels Satzung Spezifika der Verarbeitung zu regeln. Dies kann jedoch nicht für Studentendaten gelten. Daher wurde die Studierendendatenverordnung (StudDatVO) Anfang November 2005[84] erlassen.

Die Verordnung, die zunächst die zulässigerweise zu verarbeitenden personenbezogenen Daten benennt, enthält zugleich aber offene Formulierungen. Sie ist dort abschließend, wo ein bestimmter Datenkatalog erkennbar ausreichend ist, um eine bestimmte Maßnahme der Hochschule durchführen zu können. Dagegen ist sie dort offener, wo sich nicht festlegen lässt, welche Daten im Einzelfall tatsächlich erforderlich sind. Dies gilt besonders für bestimmte Verfahren von Bewerbungsgesprächen, für den Ablauf von Kunsthochschulzulassungsprüfungen sowie für Besonderheiten im Examens- und Promotionsablauf.

Im Unterschied zur bisherigen Studentendatenverordnung von 1993 enthält die neu gefasste *Studierendendatenverordnung* keinen Datenkatalog, auf dessen Ziffern bei den Regelungen zur Datenverarbeitung jeweils verwiesen wird. Vielmehr ordnet sie einer bestimmten Maßnahme konkrete Daten zu, die zum Zeitpunkt ihrer Durchführung erhoben werden können. Damit wird für die Studierenden ein höheres Maß an Übersichtlichkeit und Transparenz geschaffen. Faktisch

83 JB 2004, 4.5.1
84 GVBl., 720

unverändert übernommen wurden die Regelungen zum Studierendenausweis, der auch in Form eines mobilen, personenbezogenen Datenverarbeitungssystems (z. B. einer multifunktionalen *Chipkarte*) ausgegeben werden kann. Darüber, für welche Zwecke eine solche Chipkarte genutzt werden darf, sind die Studierenden zu informieren. Hier ist für die Hochschulen künftig ein Gestaltungsspielraum eröffnet.

Handlungsbedarf seitens der Hochschulen in Berlin besteht im kommenden Jahr für den Erlass von Satzungen. Besonders scheinen hier Satzungen zur Durchführung der Evaluationsverfahren erforderlich. Das Evaluationsverfahren der Lehre war im alten Berliner Hochschulgesetz (BerlHG) klar geregelt. Um den Hochschulen hier eine größere Flexibilität zu erlauben, war es Absicht der Senatsverwaltung, die Modalitäten der Evaluation den Hochschulen zu überlassen. Dazu wurde den Hochschulen in § 6 b Abs. 3 BerlHG eine Frist bis zum 31. Dezember 2006 gesetzt. Innerhalb dieser Frist soll zunächst nach den alten Regelungen weiterverfahren werden, auch wenn sie explizit aufgehoben sind.

Nachdem die Verarbeitung der Daten Studierender transparenter als bisher geregelt wurde, müssen nun die Hochschulen durch Satzungen Festlegungen für die *Evaluation der Lehre* treffen.

Staatliche *Ethikkommission* bewertet *Arzneimittelstudien*

Als erstes Bundesland richtete Berlin per Gesetz eine Staatliche Ethikkommission zur Bewer-tung und Genehmigung klinischer Arzneimittelstudien ein[85]. Die Ethikkommission war notwendig geworden, da sich die Bestimmungen des Arzneimittelgesetzes über den Schutz des Menschen bei klinischer Prüfung eines Arzneimittels grundlegend geändert und verschärft haben. Klinische Prüfungen dürfen nur begonnen werden, wenn diese Staatliche Ethikkommission die Studie im Rahmen eines Verwaltungsverfahrens unter Beachtung enger Fristen zustimmend bewertet hat. Sie nimmt damit als staatliche Behörde hoheitliche Aufgaben wahr. Die Genehmigung ist nunmehr vom so genannten „Sponsor“ – das sind neben Ärzten vor allem forschende Pharma-Unternehmen – zu beantragen.

Die Ethikkommission, der nicht nur Mediziner, sondern auch Pharmazeuten, Bio-Statistiker, Juristen sowie Laien ehrenamtlich angehören, besteht aus mehreren Ausschüssen. Wenn Probanden für die Teilnahme an klinischen Studien gewonnen werden sollen, sind hohe Anforderungen insbesondere an die Einwilligungserklärung, an die Information über das Verfahren, aber auch über Nebenwirkungen, und – datenschutzrechtlich am relevantesten – an die Erhebung, Verarbeitung

85 GVBL 2005, 466

und Übermittlung der personenbeziehbaren Daten der Probanden zu beachten. Das Arzneimittelgesetz schreibt darüber hinaus eine Verpflichtung zur Pseudonymisierung vor[86]. Hierfür gilt es sichere Verfahren zu entwickeln.

Da auch in den anderen Bundesländern solche Staatlichen Ethikkommissionen per Gesetz zu bilden sein dürften, stellt sich insbesondere für die „Sponsoren“ das Problem, dass die inhaltlichen, aber vor allem auch die datenschutzrechtlichen Anforderungen an das Verfahren, die Information und die Einwilligung einheitlich zu handhaben sind. Daher sollte die Staatliche Ethikkommission des Landes Berlin die Initiative ergreifen und einen bundesweiten Arbeitskreis der Länder-Ethikkommissionen gründen. Der bisherige Arbeitskreis, der bislang 96 verschiedene Ethikkommissionen umfasste, die bei den Universitätsklinika bzw. den Ärztekammern angegliedert waren, konnte dieses Ziel in der Vergangenheit nicht erreichen. Da es sich nunmehr aber um ein staatliches Genehmigungsverfahren handelt, ist dies dringend erforderlich. Die datenschutzrechtlichen Aspekte einheitlicher Vorgaben sollten parallel dazu im Arbeitskreis „Wissenschaft“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingehend beraten werden.

Neben der Vereinheitlichung der Anforderungen an klassische Medikamentenstudien geht es auch um einheitliche Anforderungen an Biobanken, in denen genetisches Material gespeichert wird. Hier hat der Arbeitskreis „Wissenschaft“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gemeinsam mit der *Telematik-Plattform für Medizinische Forschungsnetze* (TMF) eine wesentliche Vorarbeit geleistet. Die TMF konnte im Oktober 2005 ein generisches Konzept für *Biobanken* vorlegen, das aber noch einer abschließenden Überarbeitung bedarf. Im Zentrum stehen dabei Anforderungen an eine mehrstufige Pseudonymisierung der medizinischen Daten und Proben.

Die Ethikkommissionen der Länder sollten sich auf einheitliche Kriterien für die Genehmigung von Forschungsvorhaben verständigen. Auch die Datenschutzbeauftragten streben eine einheitliche Beratung der Datenschutzaspekte solcher Vorhaben an.

Datenschutzgerechte *Forschung*

Wie in jedem Jahresbericht wollen wir hier eine Auswahl von Forschungsprojekten kurz vorstellen, für die es mit zum Teil erheblichem Beratungsaufwand gelang, einen optimalen Datenzugang für die Forscher zu ermöglichen und zugleich die Rechte der Betroffenen auf informationelle Selbstbestimmung zu wahren.

Von Forschern befragt wurden:

86 vgl. dazu 3.4

- Schüler, Eltern und Lehrer im Rahmen einer Internationalen Studie zur Entwicklung von Ganztagsschulen, die als Längsschnitt bis zum Jahr 2008 durchgeführt werden soll,

- Schüler der 7. Klassen zum Gesundheitsverhalten,

- Schüler und Lehrer zu Lernstrategien,

- Schüler und Eltern vor und nach dem Schulwechsel in die Sekundarstufe I,

- Schüler von Hauptschulen zu ihrer „sozialen Identität“,

- Schüler im Rahmen einer WHO-Studie zum Gesundheitsverhalten,

- Jugendliche mit Migrationshintergrund zur Wirksamkeit von Fördermaßnahmen,

- Bürger vietnamesischer Herkunft zu deren Gesundheitsversorgung,

- Strafgefangene zu ihrer Sozialisation und Devianz sowie Statussituationen im Lebenslauf, insbesondere bei *Sexualstraftätern*,

- Sexualstraftäter in einer Vergleichsanalyse mit der Situation in Griechenland,

- Gefangene in Justizvollzugsanstalten zum Thema „Gewalt in Justizvollzugsanstalten“ in einer Vergleichsanalyse Österreich – Bundesrepublik Deutschland,

- Eltern von Kindern in Integrationskindertagesstätten zu ihrer Meinung zur gemeinsamen Bildung und Erziehung behinderter und nicht behinderter Kinder,

- Mieter in Hochhaussiedlungen zur empfundenen und erlebten Kriminalität,

- politisch motivierte Extremisten in *Justizvollzugsanstalten* zu ihrer Biographie.

Akteneinsicht nahmen Forscher in:

- Vergleichsarbeiten im Fach Mathematik von Schülern der 2. Klasse zur Analyse auf Verdachtsmomente für Dyskalkulie,

- Auszüge des Bundeszentralregisters zur Analyse eines möglichen Zusammenhanges von kindlichen *Opfererfahrungen* sexueller und psychischer Gewalt und späterer Straffälligkeit,

- statistische Daten zu Todesursachen von Patienten mit Herzschrittmachern,

- Ergebnisse eines Daten-Matchings zur Evaluation der Effizienz von Drogenkonsumräumen,

- staatsanwaltschaftliche Akten von „Intensiv-Tätern“,

- archivierte Narkose-Protokolle von Frauen mit Kaiserschnittentbindungen,

- *Personalakten* Westberliner Bauräte, die den Wiederaufbau nach dem 2. Weltkrieg organisierten,

- medizinische Unterlagen zur Schlaganfall-Forschung,

- *Gefangenenpersonalakten* von Sexualstraftätern, die testosteronsenkende Medikamente einnehmen, im Vergleich zu einer Kontrollgruppe,

- Unterlagen aus medizinisch-psychologischen Untersuchen zur Ermittlung von Falschprognose-Quoten,

- eine spezielle Datenbank bei dem Landeskriminalamt, um Vorschläge für eine wissenschaftlich fundierte Umorganisation zu unterbreiten,

- Unterlagen verstorbener Mitarbeiter des ehemaligen „Radio Berlin International“.

Darüber hinaus haben wir Forscher zu folgenden Themen beraten:

- zur wissenschaftlichen Nutzung und Archivierung von Abschlussarbeiten,

- zur Schaffung eines Akromegalie-Registers,

- zur Schaffung eines Registers für neuroendokrine gastrointestinale Tumoren,

- zur Probandenwerbung für medizinische Studien,

- zur Evaluation einer möglichen Nutzung von Alkohol-Interlock-Geräten für die Erteilung einer Fahrerlaubnis mit Beschränkung,

- zur Pseudonymisierung bei *Pharma-Studien*,

- zum Aufbau einer Probendatenbank im Deutschen Ressourcenzentrum für Genomforschung,

- zur Vorbereitung der Lese-Rechtschreib-Untersuchung IGLU sowie der PISA-Studie 2006,

- zur Evaluation eines „trägerübergreifenden persönlichen Budgets“ der Sozialhilfe,

- zur Analyse des Mathematik-Unterrichtes und der Nutzung von *Videoaufzeichnungen*,

- zur Durchführung einer Dunkelfeld-Studie zum sexuellen *Kindesmissbrauch*,

- zur Entwicklung eines Ausbildungsvideos für Kita-Erzieherinnen,

- zu einer Studie zu Verbreitungswegen sexuell übertragbarer Krankheiten,

- zur Durchführung einer Studie zur Geschichte der *Volkszählung* 1983/1987.

Unser Ziel ist es schon seit Jahren, durch das Mitwirken an verschiedenen Fachtagungen oder -veranstaltungen einen Schneeball-Effekt in der Beratung zu erreichen. Daher beteiligten wir uns mit einem umfassenden Beitrag an einer Fachtagung des Robert-Koch-Institutes zu Rekrutierungs-strategien bei epidemiologischen Studien. Die „Lange Nacht der Wissenschaften“ am 11. Juni 2005 nutzten wir das zweite Jahr in Folge, um gemeinsam mit dem Qualitätssicherungsregister in der Nierenersatztherapie „QuasiNiere“ in der Charité, Campus Virchow-Klinikum, Besuchern und Fachleuten Probleme der Anonymisierung und Vorteile der Pseudonymisierung nahe zu bringen.

Die Beratung von Wissenschaftlern bei der datenschutzgerechten Gestaltung ihrer Forschungsvorhaben war erneut ein Schwerpunkt unserer Tätigkeit.

***Datenfischzug* für die Diagnose *betrieblicher Gesundheit*?**

Gesundheitsförderung, Gesundheitsmanagement und Prävention sind Begriffe, die insbesondere auch durch die demographischen Prozesse der Alterung der Bevölkerung und damit auch der arbeitsfähigen Bevölkerung zunehmend mit Aktivitäten ausgefüllt werden. Bekanntlich hat die letzte Bundesregierung den Entwurf eines Präventionsgesetzes eingebracht, das u. a. auch die Arbeitgeber zu einer Reihe von Maßnahmen verpflichten sollte[87]. Dieser Gesetzentwurf ist an der Diskontinuität, d. h. am vorzeitigen Ende der Legislaturperiode, gescheitert. Der Bundesrat hatte etliche Einsprüche erhoben.

Gleichwohl bemüht sich eine Reihe von Arbeitgebern in Zusammenarbeit mit Betriebs- und Personalräten, in ihren Unternehmen und Behörden ein Klima der „betrieblichen Gesundheit“ zu schaffen. So auch eine Berliner Universität, in der zu diesem Zweck eine Mitarbeiterbefragung durchgeführt wurde. Der Fragebogen enthielt 165 mehr oder weniger gesundheitsbezogene Aussagen, die die Mitarbeiter in fünf Schritten von „Trifft nicht zu“ bis „Trifft völlig zu“ auf ihre eigene Arbeits- und Gesundheitssituation bezogen zu bewerten hatten. Einige Beispiele:

„Persönliche Initiative und Engagement sind gefragt.
Mit der Bezahlung bin ich zufrieden.
Von meinen Vorgesetzten werde ich unfair behandelt.
Wer Probleme anspricht, macht sich schnell unbeliebt.
Ich habe leicht Zugang zu meinem Vorgesetzten.
Rauchen Sie?
Es kommt vor, dass ich mich von vorgesetzten Kollegen körperlich bedrängt fühle.
Meine Arbeit wird durch Bürokratie und Formalitäten sehr eingeschränkt.
Ich habe Angst, in nächster Zeit arbeitslos zu werden.
Ich fürchte, auf einen schlechteren Arbeitsplatz zu kommen.
Mein Arbeitsplatz ist kalt.
Die Belüftung ist häufig nicht ausreichend.
Ich muss lange stehen.
Ich habe Konzentrationsstörungen.
Ich bin oft erkältet.
Nach der Arbeit kann ich nicht abschalten.
Ich fühle mich häufig überfordert.
Ich reagiere gereizt.
Es gibt Tage, da freue ich mich über meine Arbeit.“

Zur Person wurden das Alter in Fünfjahresgruppen, das Geschlecht, die Art der Arbeitszeit sowie

87 BT-Drs. 15/4833

zu betreuende Kinder und der Status „alleinerziehend“ erfragt, ebenso wie das befristete oder unbefristete Beschäftigungsverhältnis, die Zuordnung zum Überhang und die Dauer der Betriebszugehörigkeit. Um die Daten dann bestimmten Bereichen zuzuordnen, wurde eine Untergliederung nach Referaten, sonstigen Abteilungen und Instituten vorgenommen. Des Weiteren wurde der Status an der Hochschule, beispielsweise Hochschullehrer, studentischer Beschäftigter oder Lohnempfänger, erfragt. Auch wenn diese Daten ohne den Namen des Beschäftigten erhoben wurden, weisen sie auch bei einem nur geringen Wissen um die Strukturen dieser Universität ein hohes Deanonymisierungspotenzial auf; insbesondere wenn Geschlecht, Alter, Beschäftigtenstatus und Referat bzw. Institut zusammengeführt werden.

Dies haben sowohl der Personalrat als auch die behördliche Datenschutzbeauftragte im Vorfeld kritisiert. Mit der Durchführung hatte die Universität ein Unternehmen beauftragt, das seit einigen Jahren derartige Untersuchungen durchführt. So empfahl man insbesondere, die Altersgruppen und die Referate bzw. Institute stärker zusammenzufassen. Das externe Befragungsunternehmen erklärte, dass es nur Struktureinheiten benannt habe, die mehr als 20 Mitarbeiter aufweisen, ansonsten seien sie schon im Vorfeld mit anderen zusammengefasst worden. Ebenso soll bei der Auswertung verfahren werden. Ein Abgleich nach Altersgruppen war im Vorfeld nicht erfolgt.

Im Anschreiben zum Fragebogen wurde zwar zum einen auf die Freiwilligkeit hingewiesen; zum anderen wurde erklärt, dass bei der Auswertung die Ergebnisse zu Struktureinheiten zusammengefasst werden, wenn diese mit mehr als 20 Mitarbeitern besetzt sind. Unzureichend wurde den Befragten die Methodik der Auswertung dargelegt. Obwohl Personalrat und behördliche Datenschutzbeauftragte ihre Kritik fast anderthalb Monate vor dem Beginn der Erhebung geäußert hatten, wurde auf die Kritikpunkte nicht eingegangen, so dass wir dies kurz vor der Befragung kritisierten. Es entstand somit die datenschutzrechtlich missliche Lage, dass zunächst Daten erfasst werden, die dann in der Auswertung erst aggregiert und in ihrer Darstellung vergröbert werden müssen, aber als Einzeldatensätze weiterhin detailliert vorliegen. Diese Einzeldatensätze sollen dann auch mit anderen entsprechenden Datensätzen aus ähnlichen Befragungen bei dem Unternehmen zu einem Datenpool zusammengefügt werden. Das befragende Unternehmen behielt sich also vor, diese Datensätze ohne zeitliche Befristung aufzubewahren. Selbst wenn dann der Bezug zum Referat bzw. Institut gelöscht wird, bleibt ein nicht unbeträchtliches Restpotenzial der Deanonymisierung, so dass im datenschutzrechtlichen Sinne noch personenbeziehbare Daten vorliegen.

Wir prüften das betreffende Unternehmen nach der Erhebung und zu Beginn der Auswertung. Dabei machten wir ihm deutlich, dass es wegen der Personenbeziehbarkeit der erhobenen Daten in jedem Fall dem Datenschutzrecht unterliegt. Das Unternehmen arbeitet nach § 30 BDSG, denn es erhebt und speichert personenbezogene Daten, um sie in anonymisierter Form zu übermitteln.

Diese Vorschrift regelt das Verfahren für die Markt- und Meinungsforschung, worunter auch Befragungen zum Gesundheitszustand und zur Gesundheitsförderung fallen. Nach diesen Grundsätzen arbeitende Unternehmen haben die Daten, die einen Personenbezug erlauben, getrennt von den inhaltlichen Merkmalen zu speichern. Da das Unternehmen bislang die erhobenen Daten - zu Unrecht - als „anonym“ einstufte, sah es keine Notwendigkeit, seinen Meldepflichten sowie der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nach dem Bundesdatenschutzgesetz nachzukommen.

Ungeachtet dieser Mängel hatte sich ein gutes Drittel der Mitarbeiter an der Befragung beteiligt, so dass noch auswertbare Ergebnisse zu erwarten sind. Sicher wäre die Beteiligung höher gewesen, wenn die Mitarbeiter deutlicher über die Methodik der Auswertung aufgeklärt gewesen wären. Bei der Auswertung kommt es, so legte uns das Unternehmen dar, nicht auf die Beantwortung der einzelnen Frage konkret an: Diese Antworten werden in Gewichtungsnoten umgewandelt, die sich dann in zusammengefassten Indizes darstellen. Dieses Verfahren ist datenschutzrechtlich nicht zu kritisieren. Zu bemängeln ist jedoch vor allem, dass die Einzeldatensätze bezüglich der Angaben zur Person bei der Erhebung eine Detailliertheit aufweisen, die erst in der Auswertung durch Zusammenfassungen und Vergröberungen bereinigt wird. Als vertrauensbildende Maßnahme haben wir empfohlen, dass alle Auswertungen vor der Übergabe an die Universität der behördlichen Datenschutzbeauftragten vorgelegt werden, damit diese Hinweise geben und Stellung nehmen kann.

Gerade die so genannten soziodemographischen Daten bieten auch bei einer Erhebung ohne unmittelbare Identifikatoren wie dem Namen die Möglichkeit der *Deanonymisierung*. Eine gut vorbereitete Erhebung berücksichtigt dies schon im Vorfeld der Erhebung.

4.6.2 Statistik

Hartz IV und Lücken in der Statistik

Durch das Sozialgesetzbuch – Zweites und Zwölftes Buch (SGB II und das SGB XII) wurde die *Sozialleistungsstatistik* neu geregelt. In den alten Regelungen des Bundessozialhilfegesetzes (BSHG) wurde eine Bundesstatistik angeordnet, die die Statistischen Landesämter durchzuführen haben. Bundesergebnisse stellte das Statistische Bundesamt zusammen. Die Statistischen Landesämter waren somit in der Lage, detaillierte, regional und sachlich tief gegliederte Aussagen zur Sozialhilfe zu treffen.

Das neue SGB II beauftragt nunmehr die Bundesagentur für Arbeit (BA), aus den Einzeldaten Statistiken zu erstellen und zu veröffentlichen. Damit werden die Statistiken aus der Arbeits-

förderung nach SGB II und SGB III zusammengeführt. Zugleich wird im SGB XII eine Bundesstatistik zur Sozialhilfe nach neuem Recht angeordnet. Diese Bundesstatistik zur Sozialhilfe wird nach wie vor von den Statistischen Landesämtern durchgeführt. Es ergibt sich damit das Problem, dass auf der einen Seite Einzeldatensätze der Arbeitslosenstatistik und der Grundsicherung für Arbeitsuchende bei der Statistikstelle der BA und auf der anderen Seite die „Rest-Sozialhilfe-Statistik“ bei den Statistischen Landesämtern geführt werden.

Um entsprechend den regionalen Informationsbedürfnissen tief gegliederte Angaben zu erhalten, ist es erforderlich, dass die BA den Statistischen Landesämtern Einzeldatensätze zur Verfügung stellt; dafür gibt es jedoch gegenwärtig keine rechtliche Befugnis. Zur Lösung dieses Problems hat sich bei der BA ein „Expertenkreis Statistik“ gebildet, an dem sich neben einigen Statistischen Landesämtern und Ministerien einzelner Bundesländer auch der Bundesbeauftragte für den Datenschutz und wir beteiligt haben. Es wurde Einvernehmen erzielt, dass schnellstmöglich eine Rechtsvorschrift geschaffen werden sollte, die es der BA erlaubt, Einzeldatensätze – insbesondere auch mit dem Merkmal der Zugehörigkeit zur Bedarfsgemeinschaft – in pseudonymisierter Form den Statistischen Landesämtern zu übermitteln, so dass diese in der Lage sind, tief gegliederte Aussagen nicht nur zu den verbleibenden Sozialhilfedaten, sondern insbesondere auch zusammengeführt mit den Daten von *ALG II-Empfängern* zu treffen. Ein ent-sprechender Formulierungsvorschlag wurde von unserer Behörde erarbeitet und zur Diskussion gestellt.

Zur Erstellung einer aussagekräftigen Statistik über Sozialleistungen muss die *Bundesagentur für Arbeit* die Befugnis erhalten, den Statistischen Landesämtern die erforderlichen Daten zur Verfügung zu stellen.

Integrierte Gesundheits- und Sozialberichterstattung

Mit dem vom Senat beschlossenen Entwurf eines Gesetzes über den *Öffentlichen Gesundheits-dienst* wurde eine Regelung zur integrierten Gesundheits- und Sozialberichterstattung vorge-schlagen. Dabei sollen verschiedene Daten – insbesondere sozialraumbezogen, - verdichtet und zu Basisindikatoren zusammengefasst werden. Eine Voraussetzung dafür ist, dass die genutzten Daten als Einzeldaten oder wenigstens tief regionalisiert vorliegen. Dabei handelt es sich um statistische Daten, die nach dem Landesstatistikgesetz der *statistischen Geheim-haltung* unterliegen – selbst wenn sie keinen unmittelbaren Personenbezug, beispielsweise durch Namen und konkrete Adressen, mehr enthalten.

Daher legt der Gesetzentwurf fest, dass die mit der integrierten Gesundheits- und Sozial-berichterstattung beauftragte Organisationseinheit in der Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz

organisatorisch, personell und räumlich von anderen Organisationseinheiten zu trennen ist. Es handelt sich dabei um eine Statistikstelle, die der amtlichen Statistik zugerechnet wird, auch wenn sie nicht im Statistischen Landesamt bzw. im zukünftigen Amt für Statistik Berlin-Brandenburg integriert ist. Diese Statistikstelle wertet insbesondere die Daten der Schuleingangs- und -entlassungsuntersuchungen, die Sozialstatistiken nach dem Zweiten, Dritten und Zwölften Buch des Sozialgesetzbuches und dem Asylbewerberleistungsgesetz sowie Angaben zur Gesundheitsförderung und -prävention aus. Die Daten sind der Statistikstelle als Statistiken aus dem Verwaltungsvollzug durch die Dienststellen des Landes Berlin, aber auch vom Statistischen Landesamt bereitzustellen. Die Übermittlung von Namen, genauen Adressen sowie dem Geburtsag ist dabei unzulässig. Die Vorgaben des Landesstatistikgesetzes, insbesondere zur statistischen Geheimhaltung der Einzeldatensätze, sind einzuhalten.

Klarstellend wurde zudem eine Strafvorschrift in das Gesetz über den Öffentlichen Gesundheitsdienst aufgenommen, die das Zusammenführen von Einzelangaben zur Herstellung eines Personenbezuges explizit unter Strafe stellt. Um den Statistiken die nötige Transparenz und Normenklarheit zu verleihen, wird die für das Gesundheitswesen zuständige Senatsverwaltung ermächtigt, die Art der statistischen Erhebung, den Umfang der Hilfs- und Erhebungsmerkmale, die Berichtszeiträume oder -zeitpunkte und die Periodizität in einer Rechtsverordnung zu regeln.

Nach dem In-Kraft-Treten des Gesundheitsdienstgesetzes sollte eine die Statistiken regelnde Rechtsverordnung zeitnah erlassen werden.

Fusion der Statistischen Landesämter Berlin und Brandenburg

Noch im November 2005 leitete der Senat dem Abgeordnetenhaus von Berlin eine Vorlage zu, die den Entwurf eines Staatsvertrages über die Errichtung eines Amtes für Statistik Berlin-Brandenburg zum 1. Januar 2007 beinhaltet. Wir berichteten im Jahresbericht 2004[88] über die vorbereitenden Arbeiten der Projektgruppe. Datenschutzrechtlich sind – den Staatsvertrag betreffend – bestehende Probleme gelöst, so dass unsererseits keine Einwände mehr bestehen. Da der Sitz der Anstalt Potsdam sein und weitere Standorte in Berlin und Cottbus unterhalten werden sollen, ist das Sitzland Brandenburg. Daher wird klarstellend in einem Artikel des Staatsvertrages zum Datenschutz festgelegt, dass für die Verarbeitung von personenbezogenen Daten die entsprechenden Vorschriften Brandenburgs gelten und auch die datenschutzrechtlichen Bestimmungen durch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg überwacht werden. Für den im Land Berlin gelegenen Standort des Amtes kann die Landesbe-

88 vgl. 4.5.2

auftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg uns mit der Kontrolle beauftragen. Wir würden dies begrüßen.

Im Staatsvertrag findet sich eine alte, datenschutzrechtlich nicht unbedeutende Forderung berücksichtigt: Das Gemeinsame Amt für Statistik soll die Rechtsform einer rechtsfähigen Anstalt annehmen. Damit wird – insbesondere gegenüber auskunftspflichtigen Bürgern und Unternehmen – der Charakter einer Einrichtung unterstrichen, die nach den Grundsätzen der Neutralität, Objektivität und wissenschaftlichen Unabhängigkeit handelt. Ein Herauslösen dieser Anstalt aus der Rechts- bzw. Fachaufsicht der jeweiligen Innenressorts ist damit aber noch nicht verbunden.

Für eine konstruktive Beratung und Kontrolle des künftigen Gemeinsamen Amtes für Statistik der Länder Berlin und Brandenburg durch die beteiligten Datenschutzbeauftragten ist gesorgt.

Volkszählung 2010/2011

Im Koalitionsvertrag der neuen Bundesregierung ist Folgendes zu lesen:

„Deutschland beteiligt sich an der auf EU-Ebene 2010/2011 anstehenden neuen Zensusrunde, die mit möglichst geringen Belastungen für die Bürgerinnen und Bürger und so kostengünstig wie möglich durchgeführt werden soll.“

Bekanntlich wurde die letzte Volkszählung in der alten Bundesrepublik im Jahre 1987 durchgeführt. Für die ehemalige DDR gehen hier die Daten auf das Jahr 1981 zurück. Nach Empfehlungen der UNO und der EU sollten Volkszählungen im Abstand von etwa 10 Jahren durchgeführt werden. An der Volkszählungsrunde auf EU-Ebene für die Jahre 2000/2001 beteiligte sich Deutschland durch die Bereitstellung von fortgeschriebenen Daten. Insbesondere auch unter Nutzung des *Mikrozensus* als „kleiner Volkszählung“, bei der in jedem Jahr 1 % der Einwohner befragt wird, wurden stark aggregierte Daten, die jedoch den Anforderungen der EU genügten, erzeugt. Diese Daten konnten aber in keiner Weise den inländischen Bedarf nach regional und fachlich tief gegliederten Angaben befriedigen. Um dem Abhilfe zu schaffen, entwickelten die Statistiker Methoden, die es erlauben, Daten verschiedener Register (der Melderegister, der Register der Bundesagentur für Arbeit, der Rentenversicherungsträger u. a.) personenbezogen im abgeschotteten Raum der Statistik zusammenzufügen. Diese Methoden wurden auf der Grundlage eines *Zensustestgesetzes*[89] getestet und müssen für den Einsatz 2010/2011 noch weiterentwickelt werden. Eine Befragung der Bewohner als Auskunftspflichtige soll möglichst vermieden werden.

89 BGB 2001, 18

Mit dem Ergebnis der Tests stellte sich heraus, dass die Melderegister in nicht unbeträchtlicher Zahl „Karteileichen“, aber auch Fehlbestände aufweisen. Dies würde bei einer tief regionalisierten Auswertung natürlich zu Verzerrungen führen. Die Statistiker stellen daher seit längerem Überlegungen an, wie die Qualität der Melderegister verbessert werden kann („Ertüchtigung der Melderegister“), damit sie auch für volkszählungsähnliche Auswertungen geeignet sind. So können die Meldebehörden beispielsweise bei mehrfacher Unzustellbarkeit von Lohnsteuerkarten und Wahlbenachrichtigungen die betreffende Person von Amts wegen aus dem Melderegister abmelden. Wieweit solche Bereinigungen jedoch dem tatsächlichen Leben entsprechen, sei dahingestellt. Wenn also amtliche Post über einen längeren Zeitraum nicht zustellbar ist, heißt dies ohne eine Überprüfung vor Ort noch nicht in jedem Fall, dass diese Person an diesem Wohnort nicht mehr existent ist.

Es bleibt also von datenschutzrechtlicher Seite zu beobachten, wie hier Regelungen getroffen werden, die Personen auch nach längerer Abwesenheit von ihrer Hauptwohnung vor einer ungerechtfertigten Abmeldung von Amts wegen schützen. Auch von dem ab 2007 in die Melderegister aufzunehmenden einheitlichen und lebenslangen *Steuerkennzeichen* versprechen sich die Statistiker Vorteile, weil bei der Einführung einer einheitlichen Steuernummer Melderegisterbereinigungen vorgenommen werden. Dieses Kennzeichen darf jedoch nicht Eigenschaften eines einheitlichen *Personenkennzeichens* annehmen, dessen Einführung das *Bundesverfassungsgericht* als verfassungswidrig bezeichnet hat[90].

Da die Statistiker im Statistischen Landesamt wie auch in den anderen Statistischen Landesämtern und im Bundesamt aus Gründen der Akzeptanz der amtlichen Statistik bei der Bevölkerung sehr darauf bedacht sind, einen hohen datenschutzrechtlichen und technisch-organisatorischen Standard ihrer Arbeit zu sichern, stehen das Berliner Statistische Landesamt wie auch die anderen Statistischen Ämter im engen Dialog mit uns und den anderen Datenschutzbehörden.

Bei der Verarbeitung der Volkszählung 2010/2011 ist darauf zu achten, dass ein registergestützter Zensus die Vorgaben des Bundesverfassungsgerichts berücksichtigt.

4.6.3 Schule

Das Ende der *Lernmittelfreiheit* – eine datenschutzgerechte Lösung für die Praxis

90 BverfGE 65, 1

Nach der Lernmittelverordnung sind die Schülerinnen und Schüler verpflichtet, für jedes Schuljahr Schulbücher bis zu einem Betrag von 100 Euro auf eigene Kosten zu beschaffen. Die in § 3 Abs. 2 Lernmittelverordnung genannten Leistungsbezieher können eine Befreiung von diesem Eigenanteil beantragen. Zur Vermeidung von nicht erforderlichen Datenerhebungen über den Leistungsbezug in den Schulen hatten wir ein Gutscheinsystem angeregt, bei dem für die Schule weder die Art der Sozialleistung noch das leistungsgewährende Amt ersichtlich sein sollte. Der Vorschlag wurde von der Senatsverwaltung für Bildung, Jugend und Sport zwar aufgegriffen, scheiterte jedoch letztlich in der praktischen Umsetzung[91] zwischen den beteiligten Stellen. Für das Schuljahr 2005/2006 wurde daher mit der Senatsverwaltung für Bildung, Jugend und Sport unter Berücksichtigung der datenschutzrechtlichen Belange ein vereinfachtes Verfahren zur Registrierung der vom Eigenanteil befreiten Schülerinnen und Schüler abgestimmt.

Auf die Vergabe von einheitlichen Vordrucken zur Vorlage in den Schulen wurde verzichtet. Die Antragsteller hatten vielmehr den Bescheid der Leistung gewährenden Behörde in der Schule vorzuzeigen. Dabei konnten sie die für den Nachweis der Berechtigung nicht erforderlichen Angaben unkenntlich machen (schwärzen). Die vom Eigenanteil befreiten Schülerinnen und Schüler wurden in der Schule in einer Liste mit folgenden Angaben erfasst: Name, Vorname, Klasse, Berechtigung lag im Original vor, Name der Schule, Unterschrift. In der Liste wurden keine Hinweise auf die Leistungsart oder die Leistung gewährende Stelle vermerkt. Weder das Original noch eine Kopie des Leistungsbescheides verblieb in der Schule.

Zum weiteren Verfahren hatten wir folgende datenschutzrechtliche Rahmenbedingungen empfohlen:

Die Originalliste zur Registrierung der nach der Lernmittelverordnung vom Eigenanteil befreiten Schülerinnen und Schüler hat in der Schule zu verbleiben. Für Mitteilungen an Dritte (z. B. Stellen zur Kostenerstattung auf Bezirksebene) sind von der Schule nur anonymisierte Durchschriften, in denen die Namen der Schüler und Schülerinnen unkenntlich gemacht sind, zu übermitteln. Die Registrierung der Betroffenen ist in den Schulen von der Schulleitung bzw. in den Schulsekretariaten durchzuführen. Lehrkräfte sind grundsätzlich nicht mit der Registrierung zu beauftragen. Die Unterlagen sind in der Schule zentral (z. B. im Schulsekretariat) und unter Verschluss aufzubewahren. Die Aufbewahrungszeit der Unterlagen ist zeitlich zu begrenzen. Die Unterlagen sind spätestens zu Beginn des folgenden Schuljahres, zu dem eine neue Registrierung erfolgt, zu vernichten.

---

91 JB 2004, 4.5.3, S. 106

Unsere Empfehlungen wurden von der Senatsverwaltung für Bildung, Jugend und Sport aufgegriffen und den Schulen als verbindliche Vorgaben mit Rundschreiben vom 18. April 2005 mitgeteilt.

Um den praktischen Problemen vor Ort in den Schulen zu begegnen, wurde unter Wahrung der Interessen der Betroffenen und gemäß datenschutzrechtlichen Bestimmungen eine vereinfachte Form der Registrierung der vom Eigenanteil befreiten Schülerinnen und Schüler eingeführt.

Achtung Brandenburger – „Warnhinweis!“ an Lichtenrader Schulen

Einer Pressemeldung[92] war zu entnehmen, dass das Schulamt Tempelhof-Schöneberg Briefe an Lichtenrader Schulen versandt habe, um diese von der Aufnahme von (Schul-) Kindern aus Brandenburg abzuhalten. Die Briefe seien mit dem Titel „Warnhinweis“ überschrieben gewesen und hätten eine Liste der Kinder mit deren Vor- und Nachnamen sowie deren Geburtsdatum enthalten. Zur Erstellung der Liste habe sich das Schulamt von den Meldebehörden alle Umzüge zwischen Januar und Februar mitteilen lassen, um die melderechtlichen Anmeldungen überprüfen zu können.

Das Schulamt teilte uns dazu mit, dass es vom Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) – Einwohnerwesen – regelmäßig über den Zuzug schulpflichtiger Kinder aus anderen Bundesländern nach Berlin informiert werde. Zur Kontrolle der *Schulpflicht* versende das Schulamt in diesen Fällen ein Formschreiben, in dem die Erziehungsberechtigten gebeten werden, Auskünfte zur aktuellen Schulsituation ihres Kindes in Berlin zu geben. Die Anmeldung von Brandenburger Kindern der Jahrgänge 1992 und 1993 sei zu Beginn des Jahres 2005 in allen Einzelfällen zum Anlass genommen worden, um nicht nur die allgemeine Schulpflichtsituation zu prüfen, sondern auch die zusätzlichen Kriterien des bevorstehenden Überganges auf eine Oberschule im Land Berlin. In diesem Zusammenhang seien die Schulen im Bezirk Tempelhof-Schöneberg angeschrieben und zunächst allgemein über die Rechtslage und das Verfahren bei Anmeldungen für die Sekundarstufe I informiert worden. Die Schulen seien insbesondere darauf hingewiesen worden, dass die (positive) Aufnahmeentscheidung zukünftig durch den Schulleiter, die (negative) Entscheidung (z. B. Umlenkung, Ablehnung, Zuweisung) unverändert durch das Schulamt zu erfolgen habe. Zur „Wohnsitzproblematik“ sei auf die Regelungen des Gastschüler-vertrages mit dem Land Brandenburg verwiesen und bestimmt worden, dass sich das Schulamt die Annahme der Aufnahmeanträge in den Fällen vorbehalte, in denen der Antragsteller eine Grundschule in Brandenburg besucht habe oder die

92 Tagesspiegel v. 13. Juni 2005, S. 9

Erziehungsberechtigten während des Grundschulbesuches ihres Kindes in Berlin ihren Wohnsitz nach Brandenburg verlagert hätten. Die Oberschulen seien ausdrücklich darauf hingewiesen worden, dass sie die Aufnahme-anträge der Antragsteller in diesen Fällen nicht annehmen oder verarbeiten dürfen.

In einem weiteren Schreiben mit der Überschrift „Warnhinweis!“ seien die Lichtenrader Oberschulen und die Gustav-Heinemann-Oberschule über einige konkrete Einzelfälle informiert worden. In dem Schreiben seien den Schulen fünf Schüler aus Brandenburg mit Namen, Vornamen und Geburtsdatum benannt worden, die vom Schulamt Tempelhof-Schöneberg Ablehnungsbescheide erhalten haben. Die Ablehnung sei in diesen Fällen in Anwendung des mit Brandenburg geschlossenen *Gastschülerabkommens* erfolgt. Danach sei die Aufnahme von Brandenburger Schülern an einer Berliner Schule u. a. nur bei Vorliegen eines wichtigen Grundes und freien Kapazitäten (Schulplätzen) zulässig. Die Schulen seien angewiesen worden, jeden weiteren Anmeldeversuch der Erziehungsberechtigen für die genannten Kinder zurückzuweisen. In einer weiteren Gruppe seien drei Kinder mit Namen, Vornamen und Geburtsdatum benannt worden, bei denen die Angaben zu den Meldeverhältnissen vom Schulamt überprüft wurden. Die Prüfung habe ergeben, dass keine Schulpflicht der Kinder in Berlin gegeben und die Aufnahme durch eine Berliner Oberschule daher unzulässig sei.

Den vom Schulamt beigefügten Unterlagen zu Einzelfallprüfungen war zu entnehmen, dass dort die Wohnsitzangaben der Antragsteller (Kinder und ihre Erziehungsberechtigten) grundsätzlich durch Befragungen, Vorlage von Meldebescheinigungen, Auskünfte aus dem Einwohner-meldewesen usw. überprüft wurden.

Die Erhebung von personenbezogene Daten hat nach § 10 Abs. 1 i. V. m. § 6 Abs. 1 Berliner Datenschutzgesetz (BlnDSG) grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erfolgen und ist nur zulässig, wenn das BlnDSG selbst oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat. Eine Rechtsvorschrift in diesem Sinne ist § 64 Abs. 1 SchulG. Danach darf die Schulbehörde personenbezogene Daten von Schülerinnen und Schülern und ihren Erziehungsberechtigten verarbeiten (und damit erheben), soweit dies zur Erfüllung der ihr durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist.

Die Durchsetzung der Schulpflicht obliegt der Schulbehörde. In Berlin ist nach § 41 Abs. 1 SchulG schulpflichtig, wer in Berlin seine Wohnung oder seinen gewöhnlichen Aufenthalt oder seine Ausbildungs- oder Arbeitsstätte hat. Wer in Berlin keine Wohnung hat, kann unter bestimmten Voraussetzungen in eine öffentliche Schule des Landes Berlin aufgenommen werden. Die Entscheidung über die Aufnahme trifft nach § 41 Abs. 4 Satz 2 die zuständige

Schulbehörde. Wohnung in diesem Sinne ist nach § 41 Abs. 5 SchulG die Wohnung einer Person nach § 16 MeldeG, bei mehreren Wohnungen die Hauptwohnung nach § 17 MeldeG.

Für die Entscheidung darüber, ob ein Kind in Berlin schulpflichtig ist, ist es in jedem Fall erforderlich, dass die Schulbehörde Daten über den (Haupt-) Wohnsitz des Kindes i. S. d.
§§ 16, 17 MeldeG erhebt. Die regelmäßige Datenübermittlung durch das LABO an das Schulamt über den Zuzug von Kindern aus anderen Bundesländern ist nach § 26 MeldeG
i. V. m. § 3 Nr. 1 Anlage 4 Lfd.Nr. 3 DVO-MeldeG zulässig. Die Datenerhebung im Schulamt kann aber auch durch Vorlage des Personalausweises, einer Meldebescheinigung oder Anfrage beim LABO erfolgen. In keinem Fall gehört es jedoch zu den Aufgaben der Schulbehörde, die Richtigkeit der Meldedaten zu überprüfen. Die Verfolgung vermuteter Verstöße gegen melderechtliche Bestimmungen obliegt allein den Meldebehörden. Diese können vom Schulamt bei ungeklärten Meldeverhältnissen zur Prüfung der melderechtlichen Angaben hinzugezogen werden. Die Erhebung von Meldedaten zu diesem Zweck (z. B. durch weitere Befragung der Betroffenen, Vorlage von Meldebescheinigungen weiterer Familienmitglieder usw.) durch das Schulamt ist datenschutzrechtlich unzulässig.

Soweit sich das Landesschulamt zur Bestimmung des Wohnsitzes auf das Melderechtsrahmengesetz (MRRG) stützt, verkennt es, dass das MRRG keine unmittelbare Rechtswirkung in Berlin entfaltet. Es handelt sich hierbei vielmehr um eine Rahmengesetzgebung des Bundes, verbunden mit der Empfehlung an die Landesgesetzgeber, die dortigen allgemeinen Regelungen in das jeweilige Landesrecht zu übernehmen. Dies ist hinsichtlich § 12 Abs. 2 MRRG in Berlin bisher nicht erfolgt. Insofern kann die Regelung des § 12 Abs. 2 MRRG, wonach die Hauptwohnung eines minderjährigen Einwohners grundsätzlich die Wohnung des Personensorgeberechtigten ist, nicht zur Auslegung des § 17 BlnMeldeG herangezogen werden. Danach ist die Erhebung von Daten über den Wohnsitz Dritter (z. B. der Erziehungsberechtigten) zum Zweck der Überprüfung bzw. Interpretation der Wohnsitzangaben des Kindes i. S. d. § 12 Abs. 2 MRRG durch das Schulamt ebenfalls unzulässig.

Durch die Versendung des Schreibens mit der Überschrift „Warnhinweis!“ wurden den Lichtenrader Oberschulen und der Gustav-Heinemann-Oberschule personenbezogene Daten (Name, Vorname, Geburtsdatum, Zurückweisung der Anmeldeversuche usw.) der Betroffenen übermittelt. Hier mangelt es an der Erforderlichkeit der Datenübermittlung. Die Schulen waren bereits zuvor schriftlich vom Schulamt auf die allgemeine Rechtslage und Verfahrensweise hingewiesen worden. Insbesondere war ihnen somit bekannt, dass sich das Schulamt die Entscheidung über die Aufnahme von Kindern aus Brandenburg an Berliner Schulen in bestimmten Fallgruppen vorbehalten hatte. Eine Konkretisierung durch Übermittlung und damit

Bekanntgabe namentlicher Einzelfälle war daher – abgesehen davon, dass dadurch eine nicht hinnehmbare *Prangerwirkung* erzielt wurde – nicht erforderlich und damit unzulässig.

Bei ungeklärten Meldeverhältnissen (z. B. Verdacht auf Verwendung einer Scheinadresse) im Antragsverfahren auf Aufnahme an einer Berliner Schule ist nicht das Schulamt, sondern ausschließlich die Meldebehörde für die Überprüfung der Wohnsitzangaben nach §§ 16, 17 BlnMeldeG zuständig. Die Warnhinweise des Schulamtes Tempelhof-Schöneberg zur Aufnahme von Brandenburger Kindern an Berliner Schulen waren rechtswidrig.

Note Mangelhaft! - *Vergleichsarbeiten* in den zehnten Klassen

Im Vorfeld der im Mai 2005 in den zehnten Klassen geschriebenen Vergleichsarbeiten wurden die Berliner Schulen kurz vor den Osterferien von der Senatsverwaltung für Bildung, Jugend und Sport aufgefordert, zur Vorbereitung der umfangreichen Datenerfassung für alle in Frage kommenden Schüler einen Stammdatensatz mit den Merkmalen „Identifizierungsnummer, Klasse, Geburtstag (MM,JJ), Geschlecht, Herkunftssprache, Verkehrssprache zu Hause und LRS[93]“ anzulegen. Die Dateneingabe sollte über einen mit Passwort geschützten Bereich für die jeweilige Schule im Internet erfolgen und bis Ende April abgeschlossen sein. Nach Abschluss der Prüfungen in Mathematik, Englisch und Deutsch sollten die Schulen den Ausfall jeder Arbeit nachtragen. In den dazu versandten Rundschreiben wurde vorgeschlagen, dass die jeweiligen Fachkollegen das Passwort für die Schule erhalten und die Daten dann „in Ruhe zu Hause“ eintragen können.

Bei den Merkmalen im Stammdatensatz „Identifizierungsnummer, Klasse, Geburtstag (MM,JJ), Geschlecht, Herkunftssprache, Verkehrssprache zu Hause und LRS“ handelt es sich um schwach pseudonymisierte und damit um personenbezogene Daten der Schüler. Die Verarbeitung dieser Daten ist nur zulässig, wenn eine Rechtsgrundlage dies erlaubt. Bei der Suche nach einer Rechtsgrundlage ist der Zweck der Datenverarbeitung zugrunde zu legen. Vorliegend werden die Daten zur Vorbereitung und Durchführung eines schulübergreifenden Vergleichs im Rahmen der Qualitätssicherung nach § 9 Abs. 1 SchulG verarbeitet. Näheres, insbesondere zum Verfahren, zur Konzeption, Durchführung, Auswertung und Berichtslegung derartiger schulübergreifender Vergleiche, ist nach § 9 Abs. 6 SchulG in einer Rechtsverordnung zu regeln. Eine derartige Rechtsverordnung nach § 9 Abs. 6 SchulG wurde bisher von der Senatsverwaltung für Bildung, Jugend und Sport noch nicht erlassen. Eine andere Rechtsgrundlage für die Datenverarbeitung im Zusammenhang mit den Vergleichsarbeiten in den zehnten Klassen ist nicht vorhanden. Insbesondere kann die Datenverarbeitung nicht, da es sich hier um eine schulaufsichtsrechtliche Maßnahme mit

93 Lese-Rechtschreib-Schwäche

Außenwirkung handelt, auf die Regelungen zur Schulstatistik in § 65 SchulG bzw. § 16 SchulDatVO gestützt werden.

Die Eintragung der Schülerstammdaten und der Ergebnisse der Vergleichsarbeiten soll über das Internet von der Schule oder vom häuslichen Computer der Lehrer aus im Internetserver der Senatsverwaltung erfolgen. Die Vorgehensweise warf Fragen der informationstechnischen Sicherheit dieser Datenkommunikation auf.

Die Verbindung zum Internetserver erfolgt in sicherer Wiese, d. h., die Daten sind verschlüsselt und die Authentizität der kommunizierenden Systeme ist sichergestellt. Allerdings war die einheitliche Verwendung eines Passworts zur Authentisierung in der Schule vorgesehen, so dass es diverse Personen aus dem Schulpersonal gab, denen das Passwort bekannt war. Ferner hatten manche Schulen das anfangs an alle Schulen vergebene Initialpasswort nicht geändert, so dass man auch von anderen Schulen aus lesenden und schreibenden Zugriff auf die Daten haben konnte. Eine solche Vorgehensweise widerspricht allen Prinzipien des sicheren *Passworteinsatzes*, für den als Mindestanforderung gilt, dass jeder Benutzer sein eigenes, ständig geheim zu haltendes Passwort besitzen muss. Nach unseren kritischen Hinweisen wurde das Verfahren so geändert, dass jeder Benutzer ein eigenes Passwort benutzen kann, das er mit der Änderung eines ihm vom Schulleiter gegebenen Initialpassworts selbst bestimmen und später auch ändern kann.

Die Senatsverwaltung für Bildung, Jugend und Sport erklärte in der Sitzung des Unterausschusses „Datenschutz und Informationsfreiheit“ am 16. August 2005, dass im Vorfeld der Vergleichsarbeiten für das Schuljahr 2006/2007 eine Rechtsverordnung nach § 9 Abs. 6 SchulG erlassen werde.

Die Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler im Zusammenhang mit der Durchführung der Vergleichsarbeiten in den zehnten Klassen der Berliner Schulen war unzulässig. Dieser datenschutzrechtliche Missstand hätte durch eine rechtzeitige Vorabinformation des Berliner Beauftragten für Datenschutz und Informationsfreiheit, wie sie im Berliner Datenschutzgesetz im Übrigen vorgesehen ist, vermieden werden können.

Lange Lehren – Gesundheit und Leistungsfähigkeit im Lehrerberuf erhalten und fördern

Die Senatsverwaltung für Bildung, Jugend und Sport beabsichtigte, gemeinsam mit den Schulpsychologischen Beratungszentren und der IGES (Institut für Gesundheits-

und Sozialforschung GmbH) im Forschungsvorhaben „LANGE LEHREN – Gesundheit und Leistungsfähigkeit im Lehrerberuf erhalten und fördern“, das Projekt „Kompetenztraining zum Umgang mit Verhaltensauffälligkeiten von Schülerinnen und Schülern der Sekundarstufe I in Unterricht und Schule“ durchzuführen. Kurz vor dem Start des Projektes wurden wir gebeten, das Vorhaben datenschutzrechtlich zu bewerten.

Im Rahmen des Kompetenztrainings sollte in verschiedenen Haupt-, Real- und Gesamtschulen eine videogestützte Unterrichtsbeobachtung erfolgen. Die Videoaufnahmen der Unterrichtsstunden sollten von geschulten Praktikanten durchgeführt werden und als Grundlage für eine nachfolgende konkrete Unterrichtsauswertung zwischen der Trainerin/dem Trainer und der jeweiligen Lehrerin/dem Lehrer dienen. Vor den Aufnahmen im Rahmen des Trainings sollte die Durchführung der Videoaufnahmen von den Praktikanten in den betroffenen Klassen geübt werden.

Durch die *Videoaufnahmen im Unterricht* werden personenbezogene Daten der Schülerinnen und Schüler erhoben und gespeichert. Da es sich zum Teil um „verhaltensauffällige“ Schülerinnen und Schüler handelt, sind die personenbezogenen Daten als besonders sensitiv anzusehen. Durch die Verarbeitung dieser Daten wird daher in erheblichem Umfang in die Rechte der betroffenen Schülerinnen und Schüler eingegriffen. Dies gilt natürlich auch für die Durchführung von Probeaufnahmen zu Übungszwecken.

Dieser Eingriff ist bei Schülerinnen und Schülern unter 14 Jahren nur mit einer informierten, schriftlichen Einwilligung der Eltern zulässig. Schülerinnen und Schüler, die älter als 14 Jahre sind, sind im Vorfeld der Maßnahme ausführlich in einem Informationsschreiben über die näheren Umstände zu informieren. Insbesondere sind ihnen der Verwendungszweck, die Speicherdauer und die Regelungen des Zugriffs auf die Daten mitzuteilen. In jedem Fall sind die Betroffenen ausdrücklich auf die Freiwilligkeit der Teilnahme an der Maßnahme hinzuweisen.

Nicht die datenschutzrechtlichen Vorgaben behindern derartige Projekte, sondern der Umstand, dass diese von den Projektbetreibern erst sehr spät - am Ende der Projektvorbereitungen – erkannt werden.

Datenabgleich mit der *Agentur für Arbeit* zur Aktualisierung der *Ausbildungsstatistik*

Ein Abgleich der bei den Arbeitsagenturen in Berlin gemeldeten Ausbildungsplatzsuchenden mit den bei der IHK Berlin und HWK Berlin

eingetragenen Ausbildungsverhältnissen für das 1. Ausbildungsjahr ergab, dass rund 700 Jugendliche eine Ausbildung in einem anerkannten Ausbildungsberuf angetreten hatten, obwohl sie in der Statistik der Arbeitsagenturen weiterhin als Ausbildungsplatz Suchende geführt wurden. Aufgrund des erfolgreichen Datenaustausches mit der IHK und der HWK bat die Agentur für Arbeit darum, einen derartigen Datenabgleich auch mit den beruflichen Schulen in Berlin durchführen zu können.

Die Senatsverwaltung für Bildung, Jugend und Sport bat die Schulen, das Anliegen zu unterstützen und der Agentur für Arbeit Listen mit den Namen, Vornamen, Geburtsdaten, der Postleitzahl des Wohnortes der Schülerinnen und Schüler sowie deren Ausbildungsberuf und den Ausbildungsbeginn zu übermitteln. Für die Zukunft sollte dieser Datenabgleich zwischen den Schulen und der *Agentur für Arbeit* zum Zweck der Verbesserung, Zuverlässigkeit und Aktualisierung der Ausbildungsvermittlungsstatistik jährlich durch die Versendung von E-Mails erfolgen.

Die Übermittlung von personenbezogenen Schülerdaten an sonstige öffentliche Stellen (z. B. die Agentur für Arbeit) ist nach § 64 Abs. 3 Satz 2 SchulG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder eine Einwilligung der Betroffenen vorliegt. Eine schriftliche Einwilligung der Betroffenen (Schülerinnen und Schüler) in die Datenübermittlung an die Arbeitsagentur lag nicht vor. Eine Rechtsgrundlage, auf die die Datenübermittlung gestützt werden kann, ist hier ebenfalls nicht vorhanden.

Der Datenabgleich zwischen den Schulen und der Agentur für Arbeit war unzulässig. Nachdem wir die Senatsverwaltung auf diesen Umstand hingewiesen hatten, hat diese sofort reagiert und die betroffenen Schulen darum gebeten, von weiteren Datenübermittlungen abzusehen. Die Agentur für Arbeit wurde gebeten, die schon übermittelten Daten nicht zu verwenden und zu vernichten.

Mit der Senatsverwaltung für Bildung, Jugend und Sport wurde vereinbart, für das Schuljahr 2006/2007 eine datenschutzgerechte Lösung des Datenabgleichs zu entwickeln.

4.7 Wirtschaft

4.7.1 Verkehrsunternehmen

Deutsche Bahn AG - *Zugverspätungen* als Anlass für Datensammelei?

> *Ein Petent bat uns um datenschutzrechtliche Bewertung des von der Deutschen Bahn AG verwendeten Formulars zur Erlangung eines Ausgleichs für Verspätungen im Reiseverkehr. Unabhängig davon, ob der Fahrgast der Nutzung seiner Daten zu Kundenbetreuungszwecken bei der Deutschen Bahn AG widersprochen oder ihr zugestimmt hat, werden in dem Formular Angaben zu Namen, BahnCard-Nummer bzw. Adresse, Geburtsdatum, Datum der Zugfahrt und die Nummer des verspäteten Zuges zu Abwicklungs- und Kontrollzwecken erhoben.*
>
> *Die um Stellungnahme gebetene Deutsche Bahn AG begründete die Datenerhebung damit, zum einen ein „aktives Beschwerdemanagement“ führen zu wollen und andererseits Missbrauch mit den Gutscheincoupons verhindern zu müssen.*

Lange Zeit hat die Deutsche Bahn AG Entschädigungen bei Zugverspätungen in einem einfachen, kundenfreundlichen Verfahren gezahlt, ohne dass der betroffene Kunde dazu irgendwelche Daten preiszugeben hatte (auf seiner Fahrkarte brachte der Schaffner lediglich einen besonderen Zangenabdruck an). Erst Ende 2004 wurde dieses Verfahren in der Weise umgestellt, dass die Fahrgäste bestimmte Angaben machen müssen, um einen Gutscheinconpon zu erhalten, den sie wiederum am Schalter einlösen können.

Nachdem die Innenrevision der Deutschen Bahn AG die wachsenden Summen kritisiert hatte, die die Bahn als Entschädigung für Zugverspätung jährlich zahlt, und nachdem in den Medien über Missbrauchsmöglichkeiten berichtet wurde, die ein Professor mit seinen Studenten heraus-gefunden hatte, änderte die Bahn das Verfahren und begann, die Daten der von Verspätungen betroffenen Fahrgäste zu erheben. Seitdem verbindet sie Kontroll- mit Marketingzwecken.

Auf die Datenerhebung zu Abrechnungs- und Kontrollzwecken haben die Fahrgäste keinen Einfluss: Sie müssen sie – im Gegensatz zum früheren Verfahren – dulden, wenn sie eine Entschädigung für die Verspätung erhalten wollen. Der Nutzung der Daten zu „Kundenbetreuungszwecken“ (*Marketingzweck*) können die Fahrgäste dagegen widersprechen, was lediglich die weitere Nutzung ihrer Daten, nicht aber deren Erhebung einschränkt.

Nach Einführung des neuen Verfahrens soll die Höhe der gezahlten Entschädigungen stark zurückgegangen sein. Allerdings betrafen die beiden einzigen Fälle, in denen es bisher zu einer gerichtlichen Verurteilung wegen missbräuchlicher und betrügerischer Geltendmachung von Entschädigungsforderungen kam, Mitarbeiter der Deutschen Bahn AG.

Die generelle Erhebung personenbezogener Daten bei Zugverspätungen, wie sie die Deutsche Bahn AG neuerdings praktiziert, entbehrt, soweit sie zu Abrechnungs- und Kontrollzwecken erfolgt, jeder rechtlichen Grundlage. Lediglich die Erhebung von Fahrgastdaten zu Zwecken der Kundenbetreuung ist zulässig, wenn der Kunde sich ihr durch Widerspruch entziehen kann.

Zwar hat die Bahn ein berechtigtes Interesse daran, Missbräuche bei Vergütung für Zugverspätungen weitestgehend auszuschließen. Dies rechtfertigt aber nur dann die Erhebung personenbezogener Daten, soweit dies zur Missbrauchsbekämpfung erforderlich ist (§ 28 Abs. 1 Nr. 2 BDSG). Das ist nur denkbar in Fällen, in denen keine Einzelfahrscheine ausgegeben werden, weil der Fahrgast eine Netzkarte oder vergleichbare Zeitkarte hat.

Erst nachdem wir gegen die Deutsche Bahn AG ein Bußgeldverfahren wegen Verstoßes gegen das Bundesdatenschutzgesetz eingeleitet hatten, lenkte das Unternehmen nach dem Ende des Berichtszeitraums ein. In Zukunft können wieder alle die Kunden – wie in der Vergangenheit – Entschädigungen wegen Zugverspätungen ohne Angabe personenbezogener Daten erhalten, die einen Originaleinzelfahrschein mit einem entsprechenden Vermerk über die Verspätung vorlegen.

Die Deutsche Bahn AG hat zwar ein berechtigtes Interesse daran, den Missbrauch von Entschädigungen bei Zugverspätungen auszuschließen. Diesem Interesse ist aber auf andere Weise Rechnung zu tragen als durch die massenhafte Erhebung von Fahrgastdaten.

Speicherung in der *„Schwarzfahrerdatei“* auch ohne Missbrauch einer *Zeitfahrkarte*?

Können Inhaber von Zeitkarten bei einer Fahrkartenkontrolle ihre Zeitkarte nicht vorzeigen (so genannte Schwarzfahrt), werden ihre persönlichen Daten erhoben und bei der BVG sowie bei dem eingeschalteten Inkasso-Unternehmen, an das die Daten nach dem Vorfall übermittelt werden, gespeichert. Außerdem verlangt die BVG ein „Erhöhtes Beförderungsentgelt“, das bei nachträglicher Vorlage der Zeitkarte, der dazugehörigen Wertmarke/Wertabschnitt und/oder des gegebenenfalls erforderlichen Berechtigungs-ausweises von 40 auf 7

Euro reduziert werden kann.

Der Fahrgast ist nach § 9 Abs. 1 Satz 1 Teil A Gemeinsamer Tarif der im Verkehrsverbund Berlin-Brandenburg zusammenwirkenden Verkehrsunternehmen (VBB-Tarif) zur Zahlung eines „Erhöhten Beförderungsentgelts“ verpflichtet, wenn er sich einen gültigen Fahrausweis beschafft hat, diesen jedoch bei einer Überprüfung nicht vorzeigen kann. Das „Erhöhte Beförderungsentgelt“ in Höhe von 40 Euro (§ 9 Abs. 2 Satz 1 Teil A VBB-Tarif) ermäßigt sich auf 7 Euro, wenn der Fahrgast innerhalb einer Woche ab dem Feststellungstag bei der Verwaltung des Verkehrsunternehmens nachweist, dass er zum Zeitpunkt der Kontrolle Inhaber einer gültigen persönlichen, also nicht übertragbaren Zeitkarte oder einer entsprechenden Fahrtberechtigung war (§ 9 Abs. 3 Satz 1 VBB-Tarif, Teil A). Allerdings braucht das Verkehrsunternehmen nach § 9 Abs. 3 Satz 2 Teil A VBB-Tarif die Vorlage der Zeitkarte als Nachweis nicht anzuerkennen, wenn der Fahrgast bereits im zurückliegenden Jahr ab Feststellungstag ohne gültigen Fahrausweis oder eine entsprechende Fahrberechtigung angetroffen wurde. Diese Bedingungen differenzieren nicht zwischen Fällen, in denen ein Missbrauch denkbar ist, und solchen Konstellationen, in denen ein Missbrauch ausgeschlossen werden kann.

Petentenbeschwerden in Fällen dieser Art hatten wir zum Anlass genommen, bei der BVG darauf zu dringen, dass in Fällen, in denen ein Missbrauch bzw. eine „Schwarzfahrt“ mit Sicherheit ausgeschlossen werden kann, die Daten des Fahrgastes künftig nicht mehr in der “Schwarzfahrerdatei” gespeichert werden und eine Weitergabe an das Inkasso-Unternehmen nicht ohne vorherige “Kulanzprüfung” erfolgen sollte.

Konstellationen, in denen ein Missbrauch mit Sicherheit ausgeschlossen werden kann, sind im Bereich der so genannten persönlichen, also personengebundenen und nicht übertragbaren Zeitkarten denkbar, wie folgende Beispiele zeigen:

In den Fällen, in denen der Inhaber einer persönlichen Zeitkarte die Träger-/Kundenkarte und/oder die aktuelle Wertmarke/den aktuellen Wertabschnitt nicht bei sich führt, kann nicht mit absoluter Sicherheit ausgeschlossen werden, dass er die Zeitkarte und/oder die Wertmarke/den Wertabschnitt einem Dritten überlassen hat.

Anders sind dagegen die Fälle zu beurteilen, in denen der Inhaber einer Zeitkarte sowohl Träger-/Kundenkarte als auch Wertmarke/Wertabschnitt bei sich führt, aber die Gültigkeitsdauer der Trägerkarte bereits abgelaufen ist. Liegen die Voraussetzungen für eine Verlängerung der Kundenkarte vor, bestand z. B. zum Zeitpunkt der Kontrolle ein Ausbildungsverhältnis, ein Studenten- oder Schülerstatus, kann weder ein Dritter noch der

Inhaber selbst missbräuchlich handeln. Das gilt nicht nur für die Monatskarte für Auszubildende/Schüler (mit und ohne Abonnement, auch als Jahreskarte), die 7-Tage-Karte für Auszubildende/Schüler, das Schülerticket (mit und ohne Abonnement, auch als Jahreskarte), die Geschwisterkarte für Schüler (mit und ohne Abonnement, auch als Jahreskarte), das Semesterticket und Firmenticket, sondern auch für das neue Sozialticket und den Familienpass mit Wertmarke.

Schließlich lässt sich eine Schwarzfahrt oder ein Missbrauch mit hoher Wahrscheinlichkeit in den Fällen ausschließen**,** in denen der neben Trägerkarte und Wertmarke/Wertabschnitt zusätzlich erforderliche Berechtigungsausweis (Schüler- bzw. Studentenausweis) zum Zeitpunkt der Kontrolle nicht vorgelegt werden kann.

Selbst wenn dieser Berechtigungsausweis einem Dritten überlassen werden würde, liegt zumindest hinsichtlich der Nutzung der Beförderungseinrichtungen durch den Inhaber keine Schwarzfahrt vor, da er alle Voraussetzungen für die bei sich geführte Kundenkarte erfüllt.

Nichts anderes gilt für die Fälle, in denen der Berechtigungsausweis abgelaufen ist, aber die Voraussetzungen vorliegen, also lediglich die rechtzeitige Verlängerung versäumt wurde. Diese Fälle lassen sich auch mit den Konstellationen gleichstellen, wo die Träger-/Kundenkarte bei Vorliegen der Voraussetzungen nicht rechtzeitig verlängert wurde.

Ein Missbrauch bzw. eine Schwarzfahrt kann auch bei Fahrgästen ausgeschlossen werden, auf deren Träger-/Kundenkarte das Passfoto fehlt. In diesem Fall reicht es aus, bei der Kontrolle das lose Bild sowie den Personalausweis vorzulegen, da sich der Kontrolleur an Ort und Stelle von der Identität des Fahrgastes überzeugen kann.

“Schwarzfahren” ist kein juristischer Begriff. Gleichwohl wird das „Schwarzfahren“ umgangssprachlich häufig mit dem strafbaren „Erschleichen von Beförderungsleistungen“ (§ 265 a StGB) gleichgesetzt. Gerade darauf beruht auch die beeinträchtigende Wirkung für den Inhaber einer Zeitfahrkarte, der nur deshalb prompt in einer „Schwarzfahrerdatei“ gespeichert wird, weil er bei einer Kontrolle nicht den vollständigen Nachweis dafür erbringen kann, dass er in Wirklichkeit den Fahrpreis entrichtet hat. Er fühlt sich damit zu Unrecht als Betrüger abgestempelt.

Zwar ist auf der anderen Seite das Interesse des Verkehrsunternehmens daran anzuerkennen, dass der Fahrgast die Beweislast für die Entrichtung des Fahrpreises trägt. Dies hat seinen Niederschlag in den Beförderungsbedingungen gefunden, wonach jeder, der ohne gültigen Fahrausweis (einschließlich aller Berechtigungsnachweise) angewiesen wird, ein „Erhöhtes Beförderungsentgelt“ zu entrichten hat. Häufig dient die Einstellung der Daten solcher Personen

aber nicht nur der – berechtigten – Eintreibung dieses erhöhten Entgelts, sondern hat den Charakter einer Nebenstrafe, für die es keine Berechtigung gibt.

Speicherung der Daten

Die BVG darf nach § 3 Abs. 1 und 2 Berliner Betriebedatenverordnung (BerlBetrDatVO) (Ermächtigungsgrundlage für diese VO ist § 19 Abs. 2 Berliner Betriebegesetz) von Fahrgästen, die ohne gültigen Fahrausweis angetroffen werden, zur Beitreibung des „Erhöhten Beförderungsentgelts“ sowie zur Erfassung von Wiederholungsfällen Name, Geburtsdatum und -ort, Geschlecht des Kunden, Anschrift sowie Namen und Anschrift gesetzlicher Vertreter, Zeit, Ort und sonstige für die Rechtsverfolgung erheblichen Umstände des Vorfalls verarbeiten. Ein ungültiger Fahrausweis liegt auch in den hier interessierenden Fällen vor, in denen ein Missbrauch ausgeschlossen werden kann.

Die Erfassung von Wiederholungsfällen kann jedoch nur für “echtes Schwarzfahren” zum Tragen kommen, weil nur hier ein Interesse der BVG an der Durchsetzung ihrer Rechte besteht.

§ 3 Abs. 4 Satz 1 BerlBetrDatVO sieht jedoch für die verschiedenen Fallgestaltungen keine Unterschiede für die Löschungsfrist vor. Bei der BVG sind die zur Beitreibung des „Erhöhten Beförderungsentgelts“ sowie zur Erfassung von Wiederholungstätern erhobenen Daten ein Jahr nach Abwicklung der auf den Vorfall gegründeten Rechtswirkungen, spätestens ein Jahr nach dem letzten einschlägigen Vorfall zu löschen. Lediglich für Kinder bis 14 Jahren erfolgt die Löschung bereits nach Zahlung des „Erhöhten Beförderungsentgelts“ (§ 3 Abs. 4 Satz 2). Da bei ihnen nicht nur eine zivilrechtliche Verfolgung des Vorgangs ausscheidet, sondern wegen Strafunmündigkeit auch eine strafrechtliche Verfolgung, sind deren Daten auch nicht in die ”Schwarzfahrer- bzw. *Wiederholungstäterdatei*” aufzunehmen.

Die Frage einer Löschung nach Zahlung des „Erhöhten Beförderungsentgelts“ stellt sich auch in den Fällen, in denen ein Missbrauch ausgeschlossen ist. Eine Speicherung in der “Schwarz-ahrerdatei” bzw. Mehrfachtäter- oder Wiederholungstäterdatei ist hier nicht zulässig, da mit dieser Datei ein anderer Zweck verfolgt wird. Es bedarf einer separaten Datei mit ent-sprechender Zweckbestimmung - nämlich der Erhebung des ermäßigten „Erhöhten Beförde-rungsentgelts“ und dessen Abwicklung. Ist dieser Zweck erfüllt, müssen die Daten gelöscht werden.

Zulässigkeit der Übermittlung an ein *Inkasso-Unternehmen*

Die BVG darf außerdem die genannten Daten zur Wahrnehmung ihrer Rechte an Dritte, insbesondere an Strafverfolgungsbehörden und Inkasso-Unternehmen weitergeben. Auch in Fällen, in denen ein Missbrauch ausgeschlossen werden kann, entsteht ein zivilrechtlicher Anspruch auf das reduzierte „Erhöhte Beförderungsentgelt“, zu dessen Eintreibung sich die BVG eines Inkasso-Unternehmens bedienen darf.

Problematisch ist jedoch die sofortige Übermittlung der Daten mit dem vollen Betrag des „Erhöhten Beförderungsentgelts“ an das Inkasso-Unternehmen, da dem Kunden eine Woche Zeit eingeräumt wird nachzuweisen, dass er Inhaber einer persönlichen Zeitkarte ist, und auf diese Weise eine Reduzierung des Entgelts zu erreichen. Dieses Problem haben wir mit der BVG bereits in der Vergangenheit erörtert und die sofortige Übermittlung personenbezogener Daten noch für datenschutzrechtlich vertretbar gehalten. Allerdings haben wir ein datenschutzfreundlicheres Verhalten der BGV und einen höheren Datenschutzstandard im gesamten Verfahren angemahnt.

Einigkeit besteht damit darüber, dass die Forderung für das „Erhöhte Beförderungsentgelt“ von der BVG unmittelbar nach der Fahrkartenkontrolle an ein Inkasso-Unternehmen abgetreten werden kann. Die BVG ist deshalb nach § 3 Abs. 1 und 2 BerlBetrDatVO berechtigt, die entsprechenden Daten zur Forderungseinziehung an das Inkasso-Unternehmen weiterzuleiten.

Das Inkasso-Unternehmen ist erst nach Ablauf der Wochenfrist berechtigt, die Entgeltforderung geltend zu machen, da die Betroffenen eine Woche Zeit haben, die Forderung der BVG zu erfüllen, und bei Vorlage eventueller Nachweise erst dann die eigentliche, reduzierte Forderungshöhe feststeht. Dagegen wurde zumindest in einigen der beim Berliner Beauftragten für Datenschutz und Informationsfreiheit vorliegenden Fälle verstoßen. Es reicht nicht aus, eine ihrem Inhalt und ihrem äußeren Anschein nach als Zahlungsaufforderung zu verstehende Nachricht mit dem - klein gedruckten - Zusatz zu versehen, dass der Betroffene das Schreiben als hinfällig betrachten kann, wenn er die Forderung bereits beglichen oder sich mit der BVG in Kontakt gesetzt hat.

Das Inkasso-Unternehmen muss die ihm von der BVG übermittelten Daten unmittelbar nach Begleichung der Forderung löschen (§ 3 Abs. 4 BerlBetrDatVO). Erfolgt die Begleichung bei der BVG zusammen mit dem Nachweis der Inhaberschaft für eine persönliche Zeitkarte, muss dieser Umstand dem Inkasso-Unternehmen unverzüglich mitgeteilt werden, was wiederum eine Datenübermittlung erfordert. In den Fällen, in denen der Missbrauch von vornherein ausgeschlossen werden kann, stellt sich die Frage der Zulässigkeit einer sofortigen

Übermittlung der personenbezogenen Daten an das Inkasso-Unternehmen.

Im Ergebnis ist daher festzustellen, dass die Aufnahme und einjährige Speicherung der Daten von Personen, bei denen eine so genannte Schwarzfahrt mit hoher Wahrscheinlichkeit ausgeschlossen werden kann, unzulässig ist.

Die Rechtslage wurde der BVG ausführlich dargelegt. Das Unternehmen hat die Problematik bei Schülern erkannt und führt zurzeit ein Pilotprojekt zur Einführung eines neuen Schülerausweises durch, das im August d. J. gestartet und von unserer Behörde begleitet wird. Die voraussichtliche Dauer des Projekts beträgt ein Jahr.

Das Vorhaben der BVG, den Berechtigungsausweis und die Trägerkarte auf einem Dokument (Plastikkarte) zusammenzuführen, wird sicherlich zu einer Reduzierung von Missverständnissen und auf bloßer Nachlässigkeit beruhenden Fehlern im Umgang mit Fahrausweisen wie auch von Missbrauchsrisiken führen.

Die Berliner Verkehrsbetriebe haben sich bereit erklärt, die Fälle, in denen Missbrauch ausgeschlossen werden kann, erneut daraufhin zu überprüfen, ob sie weiterhin routinemäßig in die „Schwarzfahrerdatei“ aufgenommen werden und ein Jahr lang gespeichert bleiben sollen.

4.7.2 Banken und Auskunfteien

Basel II – *Kreditscoring*

> *Basel II ist das Kürzel für die neue Eigenkapitalübereinkunft der im Baseler Ausschuss für Bankenaufsicht versammelten Europäischen Finanzaufsichtsbehörden und Zentralbanken. Das Abkommen tritt ab dem 31. Dezember 2006 stufenweise in Kraft. Basel II ist keine Rechtsvorschrift i. S. d. § 4 Abs. 1 BDSG. Vielmehr handelt es sich um ein Verwaltungsabkommen ohne parlamentarische Ratifizierung, es wird damit gerechnet, dass das Abkommen bis Ende 2006 in nationales Recht umgesetzt wird. Basel II definiert u. a. Mindestanforderungen an die Eigenkapitalausstattung von Kreditinstituten und zielt darauf ab, die Eigenkapitalunterlegung von Krediten nicht mehr wie bisher pauschal (8 %), sondern künftig differenziert nach dem tatsächlichen Risiko vorzunehmen. Viele Banken planen allerdings, die Kreditvergabe schon im Jahre 2006 „Basel-tauglich“ zu gestalten.*

Für die Ermittlung der Eigenkapitalquote, die für einen Kredit zu hinterlegen ist, müssen die

Banken eine *Bonitätsbewertung* der Kreditnehmer vornehmen, die über die Entscheidung der *Kreditwürdigkeit* hinausgeht. Die Banken werden aber die nun zu differenzierende Eigenkapitalunterlegung zum Anlass nehmen, auch die Zinssätze für die Kreditnehmer zu individualisieren. Je höher das Bonitätsrisiko, desto höher die Zinsen.

Die Bonität der Kunden wird in der Regel durch ein Kreditscoring ermittelt. Bei der Berechnung des Score-Wertes ist insbesondere die Frage zu klären, welche personenbezogenen Daten für das Kreditscoring im Rahmen von Basel II verwendet werden dürfen. Hierfür haben wir folgende Grundsätze aufgestellt:

Es dürfen nur Parameter eingestellt werden, deren Bonitätsrelevanz mittels eines wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz des Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen Daten nur erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen danach nur Daten in ein Scoring-Verfahren eingestellt werden, die die Bank im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des Kreditwesengesetzes oder des Wertpapierhandelsgesetzes erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden.

Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Abs. 1 Satz 1 Nr. 2 BSDG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es 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. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn Banken die Möglichkeit haben, konkrete Daten zu erheben, sollten sie jedoch nicht auf Daten zurückgreifen, die nur Indizcharakter haben.

Wenn ein berechtigtes Interesse der Banken anzunehmen ist, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interesse am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen normativen Prozess dar, die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen

ist. Bei der Analyse der Generalklauseln sollte vor dem Hintergrund der Wertungen des Grundgesetzes, aber auch des einfachen Rechts, geprüft werden, ob eine Benachteiligung des Kreditnehmers aufgrund eines bestimmten Kriteriums nicht unzumutbar ist (z. B. das Scoring der Nationalität).

Auch wenn sich BASEL II vornehmlich mit der Eigenkapitalhinterlegung befasst, besteht der Sinn der Scoring-Verfahren darin, jeden Kreditvertrag entsprechend dem Risiko des Kreditnehmers zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und es sind keine überwiegenden schutzwürdigen Interessen des Betroffenen tangiert. Falls ein Scoring-Verfahren so strukturiert wäre, dass bei bestimmten Konstellationen nur „weiche Scoring-Daten“ (z. B. Wohnadresse in einem Stadtteil mit weniger zahlungskräftiger Bevölkerung) den Ausschlag für den Zinssatz geben würde, wäre ein derartiges Verfahren rechtswidrig („Verbot des Kaffeesatzlesens“).

SCHUFA-Score

Bei dem Scoring-Verfahren der SCHUFA[94] sind weitere datenschutzrechtliche Mängel erkennbar geworden. Die SCHUFA hat bei Voranschriften eine Speicherfrist von 30 Jahren festgelegt, bei mehreren Voranschriften beträgt die Frist für die letzte Wohnanschrift fünf Jahre. Dies sei für Zwecke der Identitätsfeststellung erforderlich, um Personenverwechslungen ausschließen zu können. Die Wohnanschriften werden bis zu ihrer Löschung zur Scoring-Berechnung verwendet.

Erhebt das Kreditinstitut Bonitätsdaten bei der SCHUFA, übermittelt es auf der Grundlage einer mündlichen Einwilligung das Merkmal „AK“ (= Anfrage Kredit). Die Übermittlung erfolgt insbesondere zum Nachweis des berechtigten Interesses, allerdings wird das Datum 10 Tage lang beauskunftet (um zu verhindern, dass ein Kunde mehrere Kredite gleichzeitig erhält, die kumulativ seine Zahlungsfähigkeit übersteigen). Anschließend wird das Datum ein Jahr lang zu Kontrollzwecken gespeichert und bei Selbstauskünften dem Betroffenen mitgeteilt. Das Merkmal wird bis zu seiner Löschung für das Scoring-Verfahren mit der Folge verwertet, dass sich der Score-Wert des Betroffenen verschlechtert.

Die Speicherung der Voranschriften dient ausschließlich dazu, Verwechslungen zu vermeiden. Die Voranschriften sollten deshalb spätestens nach Ablauf der in § 35 Abs. 2 Satz 2 Nr. 4 BDSG genannten Frist (regelmäßig: nach vier Jahren) nicht mehr für Scoring-Zwecke verwendet, sondern gelöscht werden. Das Merkmal „AK“ darf von dem Zeitpunkt an, wo es nur noch für

94 JB 1998, 4.6.2; JB 2000, 4.6.2; JB 2002, 4.6.2 und JB 2004, 4.6.2

Kontrollzwecke verwendet wird, nicht mehr in ein Scoring-Verfahren einfließen. Dies ergibt sich aus dem Rechtsgedanken des § 31 BDSG, wonach personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nicht mehr für andere Zwecke verwendet werden dürfen.

Das Scoring-Verfahren der SCHUFA enthält weiterhin Fehler, die die Rechtmäßigkeit des Verfahrens zumindest zweifelhaft erscheinen lassen.

Schadensrisiko* und *Bonität

> *Nach Auskunft der SCHUFA gibt es verschiedene Studien, die belegen, dass ein Zusammenhang zwischen der Bonität eines Kunden und dem Versicherungsrisiko bestehe. Personen mit schlechterer Bonität würden häufiger Versicherungsfälle verursachen. Die SCHUFA beabsichtigt, an Versicherungsunternehmen vor Vertrags-abschluss Bonitätsdaten der Versicherungsnehmer zu übermitteln, damit die Ver-sicherung die Möglichkeit hat, die Höhe der Versicherungsprämie nach der Bonität des Versicherungsnehmers zu berechnen oder bei Fehlen eines Kontrahierungszwanges eventuell auch einen Versicherungsvertrag abzulehnen. Im Ergebnis hätte es zur Konsequenz, dass jemand, der wegen einer nicht bezahlten Mobiltelefonrechnung bei der SCHUFA eingemeldet ist, höhere Versicherungsprämien für eine Hausrats-versicherung zahlen müsste.*

Ob tatsächlich der behauptete statistische Zusammenhang besteht, können wir nicht über-prüfen, weil die SCHUFA bisher keiner Aufsichtsbehörde die Studien zur Verfügung gestellt hat. Da es sich bei dem berechtigten Interesse nach § 29 Abs. 2 Nr. 1 a BDSG nicht zwingend um ein Interesse im Rahmen eines kreditorischen Risikos handeln muss, wird man den Versicherungsunternehmen ein berechtigtes Interesse an der Kenntnis der SCHUFA-Daten aber nicht von vornherein absprechen können. Allerdings übersieht die SCHUFA, dass nach § 29 Abs. 2 Satz 1 Nr. 2 BDSG kein Grund zu der Annahme bestehen darf, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Die Übermittlung der Daten erfolgt hier nicht deshalb, da der Empfänger gegenüber dem Betroffenen ein Bonitätsrisiko übernimmt und die Versicherung sich vor Vertragsverletzungen (Zahlungsausfällen) absichern will, sondern weil sich die Versicherung vor Kunden schützen will, die vertragsgemäß von dem Versicherungsschutz Gebrauch machen könnten. Die Übermittlung von Bonitätsdaten, die die Versicherung nicht vor Vertragsverletzungen schützen soll und bei der die Bonität nur mittelbar und allenfalls nach statistischen Erkenntnissen relevant ist, verletzt die schutzwürdigen Interessen der potenziellen Versicherungsnehmer.

Nach der SCHUFA-Klausel übermittelt die SCHUFA Daten an ihre Vertragspartner, um diesen Informationen zur Beurteilung der Kreditwürdigkeit zu geben. Der Betroffene kann nicht damit rechnen, dass sich das Unternehmen bei der Datenabfrage nicht für die Kreditwürdigkeit selbst interessiert, sondern ausschließlich für die sich aus der mangelnden Kreditwürdigkeit ergebende Schadensanfälligkeit.

Auch wenn ein Zusammenhang zwischen Bonität und Versicherungsrisiko bestehen sollte, ist die Übermittlung von Bonitätsdaten an die Versicherung zur Beurteilung des Versicherungsrisikos rechtswidrig.

Bonitätsauskünfte im *Vergabeverfahren*

Im Rahmen eines Vergabeverfahrens für Handwerksarbeiten hatte ein Bezirksamt Zweifel an der Bonität eines bietenden Handwerksbetriebes. Ohne Wissen des Betroffenen beschaffte sich die Vergabestelle von einer Auskunftei eine Bonitätsaus-kunft des betroffenen Handwerkers. Da diese negativ war, wurde er aus dem Vergabeverfahren ausgeschlossen.

Nicht-öffentliche Stellen haben die Möglichkeit, sich nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG Bonitätsdaten des Vertragspartners über eine Auskunftei zu beschaffen, insbesondere, wenn sie gegenüber dem Vertragspartner in finanzielle Vorleistung treten. Auch für öffentliche Stellen ist die Bonität der Vertragspartner nicht ohne Bedeutung, allerdings kommt § 28 BDSG als Ermächtigungsnorm für die Abfrage von Bonitätsdaten nur bei öffentlichen Stellen in Betracht, die am Wettbewerb teilnehmen (§ 2 Abs. 3 Satz 2 BlnDSG).

Da das Berliner Datenschutzgesetz die Datenabfrage bei einer Auskunftei nicht gestattet und der Betroffene nicht eingewilligt hat, wäre die Datenabfrage nur rechtmäßig, wenn eine besondere Rechtsvorschrift sie erlauben würde (§ 6 Abs. 1 Satz 1 BlnDSG). Gemäß § 7 Nr. 4, 5 VOL/A (nationales Vergaberecht), § 7 a Nr. 2 VOL/A (EU-Vergaberecht) hat ein Bewerber oder Bieter im Rahmen der so genannten Eignungsprüfung u. a. seine Leistungsfähigkeit darzulegen. Dazu gehört auch die Bonität des Unternehmens. Gemäß § 25 Nr. 2 Abs. 1 VOL/A darf kein Zuschlag für Angebote erteilt werden, bei denen nicht gewährleistet ist, dass die Leistung fach- und fristgerecht ausgeführt werden kann. Danach ist es die Obliegenheit eines Bewerbers oder Bieters, auch seine Bonität nachzuweisen, etwa durch eine Selbstauskunft bei einer Auskunftei. Bei Zweifeln an der Bonität des Unternehmens hat die Vergabestelle die Möglichkeit, von dem Unternehmen den Nachweis seiner Bonität zu fordern. Kommt das Unternehmen dem nicht nach, kann es vom Vergabeverfahren ausgeschlossen werden. Das Vergaberecht gibt der Vergabestelle aber nicht das Recht, hinter dem Rücken des Betroffenen Auskünfte bei Auskunfteien einzuholen. Die Vorgehensweise der Vergabestelle war mangels

Rechts-grundlage rechtswidrig.

Vergabestellen dürfen nicht hinter dem Rücken des betroffenen Bewerbers oder Bieters Bonitätsauskünfte einholen.

4.7.3 Was wir sonst noch geprüft haben …

Überwachung von Kinobesuchern mit *Nachtsichtgeräten*

> *Die Zeiten, in denen sich ein Liebespaar im Kino ungestört fühlen konnte, scheinen vorbei zu sein. Inzwischen gehen Kinos dazu über, insbesondere bei Previews und Premieren das Publikum mit Nachtsichtgeräten und Videokameras zu überwachen, um sicherzustellen, dass keiner der Gäste unter Verstoß gegen Urheberrechte Filme aufzeichnet, die dann als illegale Angebote in die entsprechenden Internetportale und Tauschbörsen gelangen. Neben der Beobachtung mit optisch-elektronischen Einrichtungen werden weitere Sicherungsmaßnahmen wie die Abgabe von Mobiltelefonen, Einsatz von Kontrollgates wie auf Flughäfen, Taschenkontrolle etc. angewandt.*

Die steigende Zahl der *Raubkopien* von Kinofilmen und der hierdurch entstandene Schaden für die Filmwirtschaft sprechen dafür, dass Kinos bei der Beobachtung von Kinobesuchern mit Nachtsichtgeräten und sonstigen Videoüberwachungen prinzipiell berechtigte Interessen wahrnehmen können, um die Erstellung von Raubkopien zu verhindern (vgl. § 6 b Abs. 1 Nr. 3 BDSG). Das berechtigte Interesse wäre allerdings in Zweifel zu ziehen, wenn sich die Vermutung bestätigen würde, dass nicht die Kinobesucher, sondern mangelnde Sicherheitsvorkehrungen bei Filmverleihern für die hohe Zahl von Raubkopien verantwortlich sind. Eine Erforderlichkeit für die Beobachtung der Kinobesucher könnte auch dann nicht angenommen werden, wenn die sonstigen Sicherheitsmaßnahmen ausreichen, um die Erstellung von Raubkopien zu verhindern. Wenn es nicht bei dem punktuellen Einsatz von Nachtsichtgeräten bleibt, sondern diese flächendeckend genutzt werden, verletzen die Kinos in der Regel überwiegende schutzwürdige Interessen der Betroffenen, die durch die Überwachungsmaßnahme unter Generalverdacht gestellt werden.

Nach § 6 b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Bei der Verwendung von Nachtsicht-geräten reicht ein bloßer Hinweis auf die Durchführung von Videoüberwachung nicht aus, da sich Kinobesucher im Fall einer bloßen Videoüberwachung in den dunklen Kinoräumen unbeobachtet fühlen könnten. Der Hinweispflicht wird somit nur Genüge getan, wenn ein Hinweis auf Nachtsichtgeräte erfolgt. Soweit Kinos mit Nachtsichtgeräten aufzeichnen, ist das Filmmaterial,

welches keine verdächtigen Handlungen von Kinobesuchern enthält, unverzüglich zu löschen (§ 6 b Abs. 5 BDSG).

Die Überwachung von Kinobesuchern mit Nachtsichtgeräten sollte auf Ausnahmefälle beschränkt bleiben, in denen konkrete Anhaltspunkte für eine besondere Gefährdung von Urheberrechten bestehen. Auf den Einsatz solcher Geräte ist unmissverständlich hinzuweisen.

PISA-Studie für Erwachsene

> *In einer Postwurfsendung werden über 40-Jährige aufgefordert, an einer „PISA-Studie für Senioren“ teilzunehmen. Es würde ein Vergleichskampf aller Bundesländer stattfinden. Dabei wird der Eindruck erweckt, die „Studie“ würde von der OECD initiiert. Abgefragt werden Wissensfragen wie Hauptstadt von Deutschland, Bundespräsident, Bundeskanzler etc. Der Teilnehmer muss Name, Anschrift, Telefonnummer und Geburtsdatum angeben. Die Unterlagen sind an ein Postfach in Berlin zu senden.*

Der Versender der Postwurfsendung täuscht vor, er würde nach den OECD-Kriterien einen PISA-Test für Erwachsene durchführen. Schon die profanen Fragen zeigen, dass keine „PISA-tauglichen“ Fragen beantwortet werden müssen. In Wahrheit geht es dem Unternehmen darum, personenbezogene Daten zu akquirieren, mit hoher Wahrscheinlichkeit für die Werbewirtschaft. Da auch die Telefonnummer abgefragt wird, liegt die Vermutung nahe, dass die personen-bezogenen Daten später auch für unerwünschte *Telefonwerbung* verwendet werden sollen (so genannte cold calls). Das Unternehmen informiert nicht über die Identität der verantwortlichen Stelle und täuscht über die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten, Daten werden somit unter Verstoß gegen § 4 Abs. 3 Nr. 1 und 2 BDSG erhoben. Für die Verarbeitung und Nutzung der durch Täuschung erlangten personen-bezogenen Daten ist keine Rechtsgrundlage ersichtlich, das Daten sammelnde Unternehmen handelt somit rechtswidrig.

Wer sich an der „PISA-Studie für Senioren“ beteiligt, hat den Test nicht bestanden.

Unzulässige Werbemaßnahme mit überraschender Begründung

> *Ein Petent hat sich in einer Eingabe darüber beschwert, von einem Unternehmen einen Anruf erhalten zu haben, der Zwecken der Werbung gedient habe. Auf seine Nachfrage,*

woher das Unternehmen seine Telefonnummer erlangt hätte, sei ihm die Auskunft erteilt worden, seine Telefonnummer sei aus einem Telefonregister im Internet bezogen worden. Uns teilte das Unternehmen mit, der Petent sei lediglich aufgrund einer Telefonumfrage zu einem „Danke-schön-Präsent“ um Erlaubnis gebeten worden, ein Produkt vorzustellen. Das Unternehmen wies darauf hin, dass, sofern der Kunde dies nicht wünsche, er nicht weiter belästigt werde.

Die telefonische Bitte an den Petenten, die Erlaubnis zu erteilen, ein bestimmtes Produkt vorzustellen, ist nach § 3 i. V. m. § 7 Abs. 2 Nr. 2 *Gesetz gegen den unlauteren Wettbewerb* (UWG) unzulässig.

Nach § 3 in Verbindung mit § 7 Abs. 2 Nr. 2 UWG ist unlauterer Wettbewerb unzulässig. Dabei handelt nach § 7 Abs. 1 UWG unlauter, wer einen Marktteilnehmer in unzumutbarer Weise belästigt. Nach dessen Abs. 2 ist eine unzumutbare Belästigung insbesondere bei einer Werbung mit Telefonanrufen gegenüber Verbrauchern ohne deren Einwilligung oder gegenüber sonstigen Marktteilnehmern ohne deren zumindest mutmaßliche Einwilligung anzunehmen (Kaltakquise, cold call).

Eine derartige Telefonwerbung verstößt im Übrigen auch gegen § 28 Bundesdatenschutzgesetz (BDSG). Sie ist gegenüber Privatpersonen nur dann als zulässig zu erachten, wenn der Angerufene zuvor sein Einverständnis erklärt hat, zu Werbezwecken angerufen zu werden. In der schriftlichen Bitte um Zusendung von Werbematerial liegt regelmäßig kein solches Einverständnis vor.

Wir haben das Unternehmen aufgefordert, künftig jegliche Art der *Telefonwerbung* ohne entsprechendes Einverständnis des Kunden zu unterlassen.

Übermittlung von *Spenderdaten* bei *Anlassspenden*

Bei Anlassspenden werden anstelle von Zuwendungen anlässlich eines Jubiläums
oder Trauerfalls Spenden zugunsten einer gemeinnützigen Organisation erbeten. Zum Beispiel wünschen sich die Angehörigen in der Traueranzeige oder in den Einladungen zu Beerdigungen anstelle von Kränzen eine Spende zu einer bestimmten Organisation. Der Spendenveranlasser vereinbart mit der Spendenorganisation ein Stichwort, wodurch die individuellen Spenden dem Anlass zugeordnet werden können. Die Spenden-organisation übermittelt dem Spendenveranlasser in der Regel die Spendenliste und die eingegangene Gesamtspendenhöhe, teilweise aber auch die Höhe der einzelnen

Spenden.

Als Rechtsgrundlage für die Übermittlung von Spenderdaten an die Spendenveranlasser kommt nicht nur § 28 Abs. 3 Satz 1 Nr. 1 BDSG in Betracht, sondern auch § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die gemeinnützigen Organisationen haben ein berechtigtes Interesse daran, die *Spendenveranlasser* durch die Übermittlung von Daten „zufrieden zu stellen“. Hierbei ist zu berücksichtigen, dass gerade in der „Branche der Spendenorganisationen“ ein harter Wettbewerb existiert. Anzuerkennen ist aber auch das berechtigte Interesse des Spenden-veranlassers, der sich möglicherweise auch in einem persönlichen Gespräch bei dem Spender bedanken möchte (insofern wäre es nicht ausreichend, wenn der Spendenveranlasser nur über die Spendenorganisation seinen Dank an die Spender weitergeben könnte). Auf der anderen Seite sind die schutzwürdigen Interessen der Spender zu berücksichtigen. Diese müssen nicht damit rechnen, dass die genaue Spendenhöhe an den Spendenveranlasser übermittelt wird. Diese ist für den Spendenveranlasser auch nicht erforderlich, um seinen Dank an die Spender zu richten, sondern dient eher der Befriedigung seiner persönlichen Neugierde.

Bei Anlassspenden dürfen Spendenorganisationen die Namen der Spender und die Gesamthöhe des gespendeten Betrages an den Spendenveranlasser übermitteln, nicht jedoch die Höhe der einzelnen Spende.

Leichtfertiger Umgang mit Kundendaten

Immer wieder stellt man fest, dass Unternehmen mit Kundendaten leichtfertig umgehen. Hier drei Beispiele:

Um zu beweisen, dass einem Kunden eine bestimmte Ware zugegangen ist, wurde ihm die ungeschwärzte „Postfrankierliste“ zugeleitet, die die Namen aller Kunden enthielt, denen an dem bestimmten Tag Waren zugesandt wurden.

Zeitungsabonnenten wurden durch eine von der Zeitung zugesandte Postkarte dazu verleitet, ihre Kontodaten auf einer Postkarte zu versenden.

Eine Bank speichert die volle Kundenadresse auf den Kontoauszügen mit der Folge, dass dieses Datum nach dem Verlust der EC-Karte leicht in falsche Hände geraten kann. Denn die Banken haben ihre bereits früher von uns kritisierte Praxis nicht verändert, noch kann jeder an Kontoauszugsdruckern allein mit der EC-karte (ohne Eingabe einer PIN) den Ausdruck eines Auszuges veranlassen.

Das erstgenannte Unternehmen hat zugesagt, zukünftig zu Beweiszwecken keine personenbezogenen Daten Dritter preiszugeben, die Zeitung wird zukünftig ihre Abonnenten darüber informieren, dass die Postkarte auch in einem verschlossenen Umschlag verschickt werden kann und die Bank plant, ihren Kunden ein Widerspruchsrecht einzuräumen, falls sie die Adressangabe auf den Kontoauszügen nicht wünschen.

Größere Sorgfalt beim Umgang mit Kundendaten sollte in jedem Unternehmen ein selbstverständliches Qualitätsmerkmal sein, ohne dass sich Kunden erst an die Aufsichtsbehörde wenden müssen.

Bestellung von Berufskleidung für Juristen über das Internet

Ein Internet-Verkäufer von Berufskleidung für Juristen erhob nicht nur den Namen, die Anschrift und die E-Mail-Adresse des Kunden, der Kunde musste außerdem für seine Bestellung Angaben über seine berufliche Tätigkeit (Richter, Staatsanwalt, Rechtsanwalt etc.) machen und darüber informieren, in welcher Dienststelle er arbeitet. Letztere Information benutzte der Verkäufer, um einem Kunden, mit dem er sich in einem zivilrechtlichen Streit befand, mit einer Dienstaufsichtsbeschwerde drohen zu können.

Ein Internet-Verkäufer darf die Daten seiner Kunden erheben und speichern, die zur Vertragsabwicklung erforderlich sind. Gegen die Erhebung und Speicherung von Namen und Adressen der Kunden bestehen danach keine Bedenken, die E-Mail-Adresse benötigt der Internet-Verkäufer schon aufgrund der Verpflichtung, den Zugang der Bestellung nach der Vorgabe des § 312 e Abs. 1 Satz 1 Nr. 3 BGB unverzüglich auf elektronischem Wege zu bestätigen. Eine über den schriftlichen und elektronischen Postweg hinausgehende Kontaktaufnahme ist allerdings nicht erforderlich. Die Angabe der Telefon- und Faxnummer des Kunden sollte deshalb freiwillig erfolgen.

Kenntnisse über die berufliche Tätigkeit und die Dienststelle des Kunden benötigt der Internet-Verkäufer nicht, um dem Kunden die gewünschte Robe zuzusenden. Es reicht aus, wenn in dem Internet-Angebot bei der Artikelauswahl auf die jeweils bestehenden Unterschiede der jeweiligen Produkte hingewiesen wird. Insbesondere ist die Verwendung der erhobenen Daten zu anderen Zwecken als der Vertragsabwicklung, etwa zur Ermöglichung dienstrechtlicher Beschwerden über die Kunden, unzulässig (vgl. § 28 Abs. 2 BDSG). Dies gilt umso mehr, da die Geltendmachung etwaiger kaufvertraglicher Ansprüche in keinem Zusammenhang zu vermeintlichen Pflichtverletzungen eines Beamten steht, welche der Dienstaufsicht unterlägen.

Bei Bestellungen über das Internet muss der Käufer nur die Daten preisgeben, die der Internet-Verkäufer für die Vertragsabwicklung benötigt.

Rabattsystem **im Supermarkt**

Bei der Kontrolle eines Rabattsystems im Supermarkt stellten wir fest, dass das Unternehmen alle Informationen auf dem Kassenbon zusammen mit den personenbezogenen Rabattkundendaten speicherte. Das Rabattsystem speicherte also nicht nur den Rechnungsendbetrag, sondern die Zahlungsart und jeden einzelnen Artikel, den der Kunde eingekauft hat. Eine Löschung der Daten wurde auch nicht nach Ausbezahlung des Rabatts vorgenommen.

Das Unternehmen beabsichtigte nicht, von seinen Rabattkunden *Käuferprofile* zu erstellen. Die Speicherung der gekauften Produkte erfolgte nur, da die gekaufte Rabattsoftware die Daten des Kassenbons speicherte. Nach dem Grundsatz der Datenvermeidung und Datensparsamkeit hätte der Supermarkt schon beim Kauf der Software darauf achten müssen, dass diese so gestaltet ist, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden (vgl. § 3 a Satz 1 BDSG). Allerdings gebietet es auch das in § 28 Abs. 1 Satz 1 Nr. 1 BDSG festgelegte Erforderlichkeitsprinzip, über Rabattkunden nur die Daten zu speichern, die für das Rabattsystem benötigt werden. Für das Rabattsystem des Kaufhauses wird nur der Rechnungsendbetrag, nicht jedoch die einzelnen Produkte, die der Kunde eingekauft hat, benötigt. Die Speicherung dieser Daten ist rechtswidrig. Das Unternehmen ist nicht berechtigt, Informationen auf dem Kassenbon zusammen mit den personenbezogenen Rabattkundendaten zu speichern.

Bei Rabattsystemen ist der Erforderlichkeitsgrundsatz schon beim Kauf der Rabattsoftware zu beachten.

Betreuung von Kunden und ehemaligen Kunden bei einem Energieversorger

Ein Energieversorger speichert von Kunden, die den Stromliefervertrag gekündigt haben, folgende Daten: Namen, Anschrift, letzten Tarif des Kunden, Vertragslaufzeit, letzten Jahresverbrauch, Namen des neuen Stromlieferanten. Der Datensatz wird von dem Unternehmen dazu verwendet, den Kunden auf den konkreten Fall bezogene Angebote zur Rückkehr zum alten Stromversorger zu machen (Kundenrückgewinnung).

Um die Kunden des Stromversorgers „bei Laune zu halten“, werden ihnen in bestimmten Abständen Broschüren zugesandt, die 12 Vorzugsangebote von Kooperationspartnern und ein Gewinnspiel enthalten. Bei einigen Tarifen ist der Erhalt der Broschüre Vertragsbestandteil, bei anderen Tarifen kann man die Broschürenzusendung beantragen. Über die eingelösten Angebote ermittelt das Unternehmen, welche Angebote von den Kunden angenommen werden; über die Couponnummer ist aber auch ermittelbar, in welchem Umfang die einem bestimmten Kunden zugesandten Gutscheine eingelöst wurden und welche Angebote für ihn insbesondere interessant waren.

Auch wenn Unternehmen nach der Beendigung von Verträgen aufgrund von gesetzlichen Aufbewahrungsfristen nicht alle personenbezogenen Daten der Kunden sofort löschen dürfen, heißt dies nicht, dass die Daten in dieser Zeit für Werbezwecke verwendet werden dürfen (vgl. § 35 Abs. 3 Nr. 1 BDSG). Die gesperrten Daten dürfen nicht mehr im operativen Geschäft, also auch nicht für Werbezwecke, verwandt werden. Insbesondere ist das Interesse, Kunden zurückzugewinnen, kein überwiegendes Interesse i. S. d. § 35 Abs. 8 Nr. 1 BDSG, wie es das Unternehmen fälschlicherweise annahm. Nach dem Rechtsgedanken des § 28 Abs. 3 Satz 1 Nr. 3 BDSG sind Unternehmen grundsätzlich berechtigt, Werbedateien auch mit Daten von ehemaligen Kunden zu erstellen, allerdings müssen sich diese Daten auf bestimmte Grunddaten wie Name, Titel, akademischer Grad, Anschrift und Geburtsjahr beschränken. Der hier verwendete Datensatz für eine optimale Bewerbung und die Erstellung maßgeschneiderter Angebote ist mangels Rechtsgrundlage rechtswidrig.

Es bestehen keine Bedenken dagegen, dass das Energieversorgungsunternehmen statistisch ermittelt, welche Angebote in der Broschüre bei seinen Kunden Interesse gefunden haben. Ob ein einzelner Kunde Gutscheine einlöst oder nicht, ist für das Unternehmen zumindest bei den Tarifen nicht relevant, die das Unternehmen zur Zusendung von Gutscheinen verpflichtet. Die Datenverwaltung sollte deshalb so organisiert sein, dass derartige Datensätze nicht erstellbar sind. Insbesondere aber muss das Unternehmen sicherstellen, dass es – anders als zurzeit – nicht in der Lage ist, über die Gutscheine Freizeitprofile seiner Kunden zu erstellen. Obwohl nicht beabsichtigt war, derartige Profile zu erstellen, ist schon die Schaffung dieser Möglichkeit rechtswidrig.

Nicht alle für die Erstellung maßgeschneiderter Angebote geeigneten Daten dürfen in einer *Werbedatei* gespeichert werden. Dies gilt insbesondere für gesperrte Daten. Schon die abstrakte Möglichkeit, Kundenprofile zu erstellen, führt häufig zur Rechtswidrigkeit der Datenverarbeitung.

Aufbau einer *Warndatei* im Einzelhandel

Ein Unternehmen beabsichtigte den Aufbau eines Brancheninformationsdienstes (Warndatei) für den Handel für Kassenkräfte, Filialleiter und andere in einer Vertrauensstellung tätige Arbeitnehmer zur Begrenzung von so genannten Inventurdifferenzen (Warenschwund durch Diebstähle).

Geplant war die Gründung einer *Auskunftei* nach § 29 Bundesdatenschutzgesetz (BDSG) sowie der Aufbau einer Warndatei, deren Ziel sein sollte, die Überprüfung von Referenzen zu automatisieren und wirksam zu verhindern, dass unehrliche Mitarbeiter beschäftigt werden. Sie sollte Einträge zu überführten (1. Fall) und geständigen (2. Fall) Mitarbeitern des Einzelhandels enthalten. Im 1. Fall sollte es ausreichen, dass ein bestimmter Verdacht gegen den Beschäftigten besteht. Von diesem sollte man sich möglichst schnell trennen können, ohne ein langwieriges Strafverfahren mit ungewissem Ausgang durchführen zu müssen, und gleichzeitig in die Lage versetzt werden, andere Arbeitgeber bzw. Kollegen wirksam zu warnen. Im 2. Fall sollte ein notarielles Schuldanerkenntnis ausreichen.

Es war vorgesehen, dass der Einzelhandel bzw. die Arbeitgeber personenbezogene Daten an die Warndatei übermitteln. Zu diesem Zweck sollten Kassenkräfte, Filialleiter und andere in einer Vertrauensstellung tätige Einzelhandelsmitarbeiter bei ihrer Einstellung in Handelsunternehmen schriftlich zustimmen, dass der Arbeitgeber im Falle des Ausscheidens Daten über die näheren Umstände der Kündigung an den Betreiber der Warndatei weitergeben kann. Die Zustimmung sollte freiwillig sein. Gegen einzelne Einträge sollte der Mitarbeiter schriftlich Widerspruch einlegen können. Der Eintrag des Arbeitgebers sollte jedoch in der Warndatei bleiben, bis eine Klärung des Einspruchs vorliegt.

Es wurde zudem in Betracht gezogen, dass Einträge in die Warndatei direkt online durch die Arbeitgeber getätigt werden, um die Bearbeitung effizienter zu machen. Die Speicherdauer sollte sich nach den Bestimmungen des Bundeszentralregistergesetzes richten.

Die Übermittlung dieser personenbezogenen Daten durch den Arbeitgeber an den Betreiber der Warndatei ist nach § 4 Abs. 1 BDSG nur zulässig, wenn das Bundesdatenschutzgesetz selbst oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene darin eingewilligt hat.

Nach § 4 a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dies ist insbesondere dann fraglich, wenn die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition eingeholt wird. Bewirbt sich ein Interessent um

einen derartigen Arbeitsplatz, wird er der Datenübermittlung an den Betreiber der Warndatei zustimmen, um nicht Gefahr zu laufen, von vornherein aus dem Kreis der Mitbewerber auszuscheiden. Die Motivation für die Einwilligungserklärung ist daher nicht als selbstbestimmt anzusehen. Bei Einwilligungserklärungen von Bewerbern um einen Arbeitsplatz in die Verarbeitung ihrer personenbezogenen Daten ist somit grundsätzlich von einer fehlenden Freiwilligkeit auszugehen. Der Arbeitgeber könnte die Übermittlung von personenbezogenen Daten an den Betreiber der Warndatei nicht auf diese Erklärung stützen.

Auch § 28 Abs.3 Nr.1 BDSG kann nicht als Rechtsgrundlage für die beabsichtigte Datenübermittlung an die Warndatei herangezogen werden. Zwar haben Dritte, hier andere Einzelhandelsunternehmen, ein großes Interesse daran, dass sie keine Beschäftigten einstellen, die bereits „auffällig“ geworden sind. Durch die Einmeldung eines Beschäftigten in die Warndatei werden andere Arbeitgeber über dessen Unredlichkeit informiert, das betriebliche Risiko wird insoweit gemindert.

Dem berechtigten Interesse des Arbeitgebers steht hier jedoch das schutzwürdige Interesse des Arbeit Suchenden am Ausschluss der Übermittlung entgegen. Die schutzwürdigen Interessen des Betroffenen müssen nach dem Verhältnismäßigkeitsgrundsatz mit denen der speichernden Stelle abgewogen werden. Insbesondere müssen Art, Inhalt und Aussagekraft der betreffenden Daten an den Aufgaben und Zwecken gemessen werden, denen ihre Verarbeitung dient. Dabei sind die Konsequenzen, die eine Datenübermittlung für den Betroffenen haben kann, zu berücksichtigen.

Nach Art. 18 der Verfassung von Berlin haben alle das *Recht auf Arbeit*. Dieses Recht zu schützen und zu fördern ist Aufgabe des Landes Berlin. Es soll zur Schaffung und Erhaltung von Arbeitsplätzen beitragen und im Rahmen des gesamtwirtschaftlichen Gleichgewichts einen hohen Beschäftigungsstand sichern. Durch den geplanten Aufbau einer Warndatei steigt das Risiko, dass Arbeit Suchende einem ungerechtfertigten Verdacht ausgesetzt werden und damit Erwerbschancen verlieren. Daher sind besonders strenge Maßstäbe an eine solche Datei anzulegen.

Die Einmeldung eines ehemaligen Beschäftigten in die Warndatei soll Daten von überführten und geständigen Mitarbeitern enthalten. Dabei kann nur derjenige als „überführt“ gelten, der rechtskräftig verurteilt ist. Dagegen ist weder ein bestimmter Verdacht, mag er auch noch so begründet oder verdichtet sein, noch ein notarielles Schuldanerkenntnis oder formloses Eingeständnis geeignet, die Schuld des Betroffenen zu beweisen. Sie müssen daher als Meldegrund ausscheiden. Befürchtete finanzielle Verluste der Einzelhändler stehen in keinem Verhältnis zu den Folgen, die den Betroffenen nach Aufnahme in die Warndatei ohne rechtskräftige

Verurteilung und nur auf der Basis von Spekulationen oder Mutmaßungen treffen. Die existenziellen Bedürfnisse eines Menschen sind in diesem Fall höher zu bewerten als das Interesse an der Begrenzung von wirtschaftlichen Schäden.

Zwar entstehen dem deutschen Einzelhandel durch unredliche bzw. kriminelle Arbeitnehmer erhebliche Schäden, das wirtschaftliche Risiko wird für den Einzelhandel jedoch nicht unkalkulierbar. Hier sind u. a. Zeugnisse geeignete Instrumente, um anderen Arbeitgebern einen Hinweis zu geben. Im Übrigen ist der gesetzlich vorgesehene Rechtsweg (Zivilklage auf Schadensersatz) zu beschreiten oder Strafanzeige zu stellen.

Eine Übermittlung der Daten an den Betreiber der Warndatei kann nach § 28 Abs. 3 Nr. 1 BDSG nur erfolgen, wenn eine rechtskräftige Verurteilung oder Vergleichbares, wie Strafbefehl bzw. Mahnbescheid, gegen den Betroffenen vorliegen. Dabei sind die Vorschriften des Bundeszentralregistergesetzes zu beachten. Auch die Speicherung von bloßen Verdachtsmomenten oder Schuldanerkenntnissen von Bewerbern in der geplanten Warndatei wäre unzulässig, da sie gegen § 29 BDSG verstieße, der die Rechtmäßigkeit dieser Maßnahme ebenfalls an die Beachtung der schutzwürdigen Belange der Betroffenen (hier der Arbeit Suchenden) knüpft.

4.8. Europäischer und internationaler Datenschutz

4.8.1 Europäische Union

Innerhalb der *Europäischen Kommission* hat sich die Zuständigkeit für den Datenschutz geändert. Die Abteilung Datenschutz, die auch das Sekretariat der Art. 29-Datenschutzgruppe beherbergt, ist inzwischen nicht mehr der Generaldirektion Binnenmarkt zugeordnet, sondern (mit unveränderten Befugnissen) der Generaldirektion Justiz, Freiheit und Sicherheit. Die neue Zuordnung kann möglicherweise als Signal für einen verbesserten Datenschutz bei der grenzüberschreitenden Kriminalitätsbekämpfung gewertet werden. Immerhin gehört auch der Grundrechtsschutz der Unionsbürger zum Aufgabengebiet der Generaldirektion Justiz, Freiheit und Sicherheit.

Erneut hat die Art. 29-Datenschutzgruppe zahlreiche Arbeitspapiere verabschiedet. Dazu gehören zwei, die sich mit der *Überprüfung von verbindlichen Unternehmensregelungen* auf ausreichende Datenschutzgarantien im Sinne von Art. 26 Abs. 2 Europäische Datenschutz-richtlinie (vgl. § 4 c Abs. 2 BDSG) befassen und an deren Entwicklung wir maßgeblich beteiligt

waren[95]. So wurde ein *Kooperationsverfahren* für die Aufsichtsbehörden festgelegt, bei dem unter Federführung einer Aufsichtsbehörde eine gemeinsame Stellungnahme aller betroffenen Aufsichtsbehörden in Europa zur Angemessenheit der Datenschutzgarantien in verbindlichen Unternehmensregelungen erarbeitet wird[96].

Zweck des Verfahrens ist, dass ein Unternehmen mit mehreren Niederlassungen in Europa nur einer Aufsichtsbehörde die verbindliche Unternehmensregelung zur Überprüfung vorlegt, obgleich Datenübermittlungen in Drittländer auf der Grundlage dieser Unternehmensregelung aus allen diesen Niederlassungen erfolgen. Maßgeblich für die Wahl der federführenden Aufsichtsbehörde ist vorrangig der Sitz der Zentrale des Unternehmens in Europa. Weitere Kriterien sind der Sitz des mit dem Datenschutz beauftragten Unternehmensteils, der Sitz des Unternehmensteils, der z. B. im Hinblick auf Managementfunktionen am besten geeignet ist, der Ort, an welchem die meisten Entscheidungen über die Datenverarbeitung getroffen werden, oder der EU-Mitgliedstaat, aus dem die meisten Übermittlungen in Länder außerhalb des Europäischen Wirtschaftsraums erfolgen.

Die Teilnahme an dem Verfahren ist freiwillig. Es bleibt abzuwarten, wie es sich bewährt. Die Aufsichtsbehörden sind sich einig, dass je nach Erfahrungen mit den in dieser Hinsicht noch offenen Testfällen[97] das Kooperationsverfahren geändert werden wird. Die britische Aufsichtsbehörde, die die Federführung bei der Anerkennung der Unternehmensregelung von General Electric (GE) Company innehat, hat den ersten Testfall fast abgeschlossen. Der vom Unternehmen vorgelegte „konsolidierte Entwurf“ wurde allen betroffenen Aufsichtsbehörden zur Stellungnahme zugeleitet[98]. Nach Beratung der eingegangenen Kommentare zwischen der britischen Aufsichtsbehörde und GE haben die Aufsichtsbehörden den „endgültigen Entwurf“ erhalten. Sie sind nun aufgerufen zu bestätigen, dass sie von der Angemessenheit der vorgeschlagenen Garantien überzeugt sind[99].

Die Art. 29-Datenschutzgruppe hat darüber hinaus für die inhaltlichen Anforderungen an Unternehmensregelungen eine *Checkliste* für die Beratung von Unternehmen auf der Grundlage der Erfahrungen der britischen Aufsichtsbehörde erarbeitet[100]. Hervorzuheben ist,

---

95 zuletzt JB 2004, 4.7.1

96 „Festlegung eines Kooperationsverfahrens zwecks Abgabe gemeinsamer Stellungnahmen zur Angemessenheit der verbindlich festgelegten unternehmensinternen Datenschutzgarantien“, WP 107 v. 14. April 2005, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 54

97 hierzu gehören die Unternehmensregelungen von DaimlerChrysler, General Electric Company und Philips, vgl. JB 2004, 4.7.1

98 vgl. Ziff. 4 im WP 107, Fn.

99 vgl. Ziff. 5 im WP 107, Fn.

100 „Muster-Checkliste für Anträge auf Genehmigung verbindlicher unternehmensinterner Datenschutzregelungen“, WP 108 v. 14. April 2005, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 43

dass das Unternehmen bei Stellung des Antrags auf Anerkennung der Unternehmensregelung der federführenden Aufsichtsbehörde Nachweise über die Verbindlichkeit der Regelungen innerhalb des Unternehmens sowie in Bezug auf die rechtliche Durchsetzbarkeit für Dritte vorlegen muss. Wesentlich ist, dass die Checkliste nur diejenigen Anforderungen umschreibt, die zur Schaffung von ausreichenden Datenschutzgarantien im Sinne von Art. 26 Abs. 2 Europäische Datenschutzrichtlinie erfüllt sein müssen. Weitergehende Anforderungen nach nationalem Recht (z. B. in Deutschland das Genehmigungserfordernis nach § 4 c Abs. 2 BDSG) sind nicht enthalten. Sie sollen in einem zusätzlichen Papier durch die jeweilige Aufsichtsbehörde dargestellt und dem Unternehmen bei Bedarf von der federführenden Aufsichtsbehörde zur Verfügung gestellt werden.

Die Art. 29-Datenschutzgruppe hielt es für erforderlich, aufgrund des rasanten technischen Fortschritts bei der Entwicklung von *RFID-Chips* und des bevorstehenden großflächigen Einsatzes dieser Technik auf mögliche datenschutzrechtliche Probleme insbesondere für Verbraucher hinzuweisen[101]. Das Konsultationspapier war Gegenstand einer öffentlichen Anhörung, an der auch Vertreter der Wirtschaft und Industrie beteiligt waren[102]. Beim Einsatz von Techniken zum *Schutz geistigen Eigentums* befürchtet die Art. 29-Datenschutzgruppe, dass die Rechte der betroffenen Nutzer in der Online-Welt nicht angemessen berücksichtigt werden[103]. Die Art. 29-Datenschutzgruppe hat sich auch mit der *Umsetzung von Art. 18 Europäische Datenschutzrichtlinie* in Europa befasst. Anders als in Deutschland sehen die meisten Mitgliedstaaten die Pflicht des Datenverarbeiters zur Meldung bei der Kontrollstelle vor. Darauf kann verzichtet werden, wenn ein interner Datenschutzbeauftragter bestellt worden ist. Der Bericht der Art. 29-Datenschutzgruppe[104] beleuchtet die unterschiedlichen Situationen in den EU-Mitgliedstaaten und enthält ein Plädoyer für die internen Datenschutzbeauftragten, das nicht zuletzt auf die Erfahrungen Deutschlands zurückzuführen ist.

Die Zusammenarbeit der Datenschutzbehörden auf europäischer Ebene gewinnt weiter an Bedeutung. Europäische und internationale Unternehmen können nur in enger Abstimmung beraten und kontrolliert werden.

4.8.2 Der datenschutzgerechte Schutz von

101 Arbeitspapier Datenschutzfragen im Zusammenhang mit der RFID-Technik, WP 105 v. 19. Januar 2005
102 Ergebnisse der öffentlichen Anhörung, WP 111 v. 28. September 2005
103 Arbeitspapier Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten, WP 104 v. 18. Januar 2005
104 über die Meldepflicht an die nationalen Kontrollstellen, zur bestmöglichen Nutzung der Ausnahmen und Vereinfachungen und zur Rolle der Datenschutzbeauftragten in der Europäischen Union, WP 106 v. 18. Januar 2005

„Whistleblowern“

Als Folge der großen Börsenskandale in den Vereinigten Staaten, die Entsprechungen auch in Europa fanden, verabschiedete der US-Kongress gesetzliche Regelungen (den sog. Sarbanes-Oxley Act von 2003), die eine Wiederholung solcher massiver wirtschaftlicher Schäden für Anleger und die Wirtschaft insgesamt erschweren sollten. So wurden die unternehmensinternen Dokumentationspflichten - auch im Interesse einer verbesserten Datensicherheit - erheblich verschärft. Die *Kapitalmarktaufsicht* und der Kampf gegen *Insiderhandel* und Kursmanipulationen wurden erheblich intensiviert.

In diesem Zusammenhang beschloss der amerikanische Gesetzgeber auch eine Regelung, nach der alle börsennotierten Unternehmen ihren Beschäftigten die Möglichkeit eröffnen müssen, einer Stelle telefonisch oder per E-mail vertraulich und anonym Hinweise auf illegale Finanztransaktionen, *Bilanzfälschungen, Korruption* oder andere Aktivitäten zu geben, die einen negativen Einfluss auf die ökonomische Lage des Unternehmens und damit dessen Börsennotierung haben können. Zugleich sollen zu diesem Zweck eingerichtete Telefon-Hotlines auch Hinweise auf unethisches Verhalten im Unternehmen (z.B. intime Beziehungen zwischen Vorgesetzten und Untergebenen, sexuelle Belästigung) entgegennehmen können. Derartige Vorkommnisse hatten in den USA zum Rücktritt eines Firmenchefs geführt.

Entscheidend ist nun, dass sich diese Verpflichtung nach US-Recht sich auch auf deutsche Unternehmen erstreckt, die an Börsen in den Vereinigten Staaten notiert sind. Wer dieser Pflicht nicht genügt, dem droht die Streichung vom Kurszettel an den amerikanischen Börsen („delisting“), was einen erheblichen Schaden für die betroffenen Unternehmen bedeuten würde.

Der gerade im angelsächsischen Rechtskreis weit verbreitete Schutz von „Whistleblowern“ (*Hinweisgebern*) ist grundsätzlich ein berechtigtes Anliegen, da auf diese Weise kriminelles, schädigendes oder unerwünschtes Verhalten bekannt und geahndet werden kann, das sonst möglicherweise nicht oder nicht rechtzeitig bemerkt würde. So sind die bei der Übernahme von Mannesmann durch Vodafone gezahlten Summen nur durch eine Whistleblowerin bekannt geworden. Insofern gehört der Schutz solcher Hinweisgeber auch im weiteren Sinne zu den Prinzipien der *Informationsfreiheit*, denn es werden Informationen zugänglich gemacht, deren Geheimhaltung nicht nur ungerechtfertigt, sondern auch schädlich sein kann. Whistleblowing kann ein Baustein zur Unterbindung von Korruption sein. Allerdings ist nicht zu verkennen, dass gerade in Deutschland ein Hinweisgeber, insbesondere wenn er auf *Anonymität* besteht, leicht in die Nähe des Denunzianten gerückt wird, zumal die jüngste deutsche Vergangenheit zahlreiche Beispiele dieses Verhaltens kennt. Bei falschen Anschuldigungen drohen den

betroffenen Personen überdies zumindest erhebliche Verletzungen ihrer Persönlichkeitsrechte.

Aus der Sicht des Datenschutzes kommt es deshalb darauf an, den berechtigten Schutz von Hinweisgebern mit der Gewährleistung des notwendigen Schutzes der Beschuldigten vor falscher Verdächtigung und seiner Rechte nach dem Datenschutzrecht (auf Auskunft, Berichtigung und Löschung) in Einklang zu bringen.

Ein zusätzliches Problem besteht darin, dass *Hotlines* zur Entgegennahme entsprechender Hinweise nicht nur innerhalb des jeweiligen Unternehmens, sondern auch von externen Dienstleistern betrieben werden können. Diese wiederum haben teilweise ihren Sitz im außereuropäischen Ausland; insbesondere bieten in den USA ansässige Unternehmen derartige Dienste europäischen Unternehmen an, die die Regelungen des US-Kapitalmarktrechts einhalten wollen. Dadurch entsteht das Problem des Datenexports in ein Drittland, in dem jedenfalls partiell kein angemessenes Datzenschutzniveau herrscht.

Nachdem die französische Datenschutzkommission (Commission Nationale de l'Informatique et des Libertés - CNIL) zunächst die Anwendung der Regeln zum Schutz von Whistleblowern in zwei französischen Tochterunternehmen amerikanischer Konzerne wegen Verstoßes gegen das französische Datenschutzgesetz untersagt hatte, begannen Gespräche zwischen ihr und der US-Börsenaufsicht (Securities Exchange Commission SEC). Die in den USA börsennotierten europäischen Unternehmen, darunter auch zahlreiche deutsche, sahen sich in dem Dilemma, einerseits den Anforderungen des amerikanischen Rechts genügen zu müssen, wenn sie weiter auf den Aktienmärkten in den USA vertreten sein wollten, andererseits aber dem europäischen Datenschutzrecht genügen zu müssen. In Deutschland erklärte das Landesarbeitsgericht Düsseldorf[105] einen unternehmensinternen Verhaltenskodex („Ethikrichtlinie") der deutschen Tochtergesellschaft des WalMart-Konzerns für unwirksam, in der Hinweisgeber auch dann geschützt werden sollten, wenn sie anonym darauf aufmerksam machen, dass Unternehmensmitarbeiter am Arbeitsplatz Liebesbeziehungen unterhalten. Eine derartige Regelung hat das LAG Düsseldorf als mit dem grundgesetzlich garantierten Persönlichkeitsrecht der Beschäftigten unvereinbar angesehen.

Auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist im vergangenen Jahr von Unternehmen immer wieder auf diese Problematik und die Notwendigkeit einer einheitlichen datenschutzrechtlichen Beurteilung in Europa hingewiesen. Er hat sich deshalb im Rahmen der Gruppe nach Art. 29 der Europäischen Datenschutzrichtlinie für die zeitnahe Ausarbeitung einen solchen Standpunkts eingesetzt. Nach dem Ende des Berichtszeitraums hat die Art. 29-Gruppe Grundsätze für die Ausgestaltung von Unternehmens-Hotlines

105 Beschluss v. 14. November 2005 - 10 TaBV 46/05 - nicht rechtskräftig

beschlossen, die die Belange des Whistleblower-Schutzes mit dem Datenschutz in Einklang bringen[106].

Danach sollen Hinweisgeber ermutigt werden, ihre Identität gegenüber der Hotline (unternehmensintern oder -extern) offen zu legen. Für diesen Fall ist ihnen Vertraulichkeit und Geheimhaltung ihrer Identität zuzusichern. Die beschuldigte Person kann nur im Fall einer wissentlich falschen Anschuldigung Bekanntgabe des Namens des Hinweisgebers verlangen. Wenn dieser allerdings darauf besteht, anonym bleiben zu wollen, ist der Hinweis zeitnah zu untersuchen. Die Entgegennahme *anonymer Anzeigen* sollte nicht der Regelfall sein, weil bei ihnen zum einen Rückfragen bei dem Anzeigeerstatter unmöglich sind, zum anderen die Möglichkeit einer Verleumdung eher besteht.

Die Art. 29-Gruppe befürwortet grundsätzlich die Einrichtung unternehmensinterner Hotlines, erkennt aber auch die Möglichkeit der Einschaltung professioneller externer Dienstleister an, wenn die zweckgebundene, zeitlich befristete Verarbeitung der häufig sensitiven Daten gewährleistet ist. Befindet sich der Dienstleister allerdings in einem Drittstaat wie den USA, muss ein angemessener Datenschutz z.B. durch die Übernahme der Grundsätze des „sicheren Hafens“ (safe harbour) gewährleistet sein.

Hinweisgeber (Whistleblower) sollten in einer Weise vor Benachteiligung geschützt werden, die die Rechte der Beschuldigten nach dem Datenschutzrecht berücksichtigt.

4.8.3 Datenübermittlung an die *Auslandshandelskammern* (AHKs)

Der Deutsche Industrie- und Handelskammertag (DIHK) mit Sitz in Berlin wollte wissen, ob und unter welchen Voraussetzungen die Industrie- und Handelskammern (IHKs) z. T. personenbezogene Unternehmensdaten (z.B. von Ansprechpartnern) an die Auslandshandelskammern (AHKs) weitergeben dürfen, die sich in Drittländern ohne angemessenes Datenschutzniveau befinden. Die AHKs geben die Daten bei konkreten Anfragen von Unternehmen im jeweiligen Staat weiter und können so zur Anbahnung von Geschäftskontakten beitragen.

106 WP 117 v. 1. Februar 2006, http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_eu.pdf

Die Weitergabe der Unternehmensdaten (auf CD) erfolgt durch die Gesellschaft für Informationsverarbeitung (GfI) mit Sitz in Dortmund im Auftrag der IHKs an die AHKs. Die Zulässigkeit dieser Datenübermittlung ist unter Berücksichtigung der im Internationalen Privatrecht gebräuchlichen „Käseglocken-Theorie“ allein nach nationalem deutschem Recht zu beurteilen. Erforderlich für den Export deutschem Rechts ist jedoch ein „deutscher Anknüpfungspunkt“ bei den AHKs, die als privatrechtliche Einrichtungen dem Recht des jeweiligen Sitzlandes unterliegen. Ein solcher ist gegeben, wenn die Mitarbeiter bei den AHKs Deutsche oder als Arbeitnehmer der IHKs beschäftigt sind. Erst in dem Moment, in dem auf Anfrage eines Unternehmens im Drittland Daten deutscher Unternehmen durch die AHKs herausgegeben werden, liegt eine Datenübermittlung ins Drittland vor, deren Zulässigkeit nach §§ 13, 14 BlnDSG zu beurteilen ist.

Wir haben dem DIHK folgende praktikable Lösung empfohlen: Nach Eingang der Anfrage bei der AHK fragt diese bei dem Unternehmen in Deutschland (per E-Mail) zurück, ob es mit der Weitergabe seiner Daten an das anfragende Unternehmen in dem konkreten Drittland einverstanden ist. Die Einwilligungserklärungen könnten vom DIHK musterhaft vorbereitet und in eine bei den AHKs befindliche Geschäftsordnung aufgenommen werden. Die Einwilligung ist nur bei denjenigen Firmen einzuholen, deren Unternehmensdaten personenbezogen sind. Diese Lösung hat folgenden Vorteil: Das deutsche Unternehmen kann im Einzelfall entscheiden, dass die Daten nur an Unternehmen in ausgewählten Drittländern herausgegeben werden, etwa weil das Unternehmen in anderen Drittländern keine Geschäfte eingehen und deshalb auch keine Daten dorthin herausgeben will. Die vom DIHK angedachte Lösung, einen Datenexportvertrag zwischen allen IHKs und allen AHKs zu schließen, ist dagegen unpraktikabel und hätte zudem als Grundvoraussetzung, dass es sich bereits um eine Datenübermittlung ins Drittland und bei den AHKs jeweils um den Datenimporteur handelt. Zudem ist gerade noch nicht bekannt, wer letztlich der Empfänger der Daten ist, da noch ungewiss ist, welche Unternehmen im Drittland tatsächlich Anfragen an die AHKs richten und daraufhin Daten erhalten.

Für die Übermittlung von personenbezogenen Unternehmensdaten über die Auslandshandelskammer in Drittländer wurde eine praktikable und datenschutzgerechte Lösung entwickelt.

4.9 Organisation und Technik

4.9.1 Behördliche Datenschutzbeauftragte

Gesprächskreis der *behördlichen Datenschutzbeauftragten* der Bezirke

Die Gesprächsrunden der bezirklichen Datenschutzbeauftragten wurden auch im Berichtsjahr fortgesetzt. Bei insgesamt vier Treffen wurden u. a. folgende Themen erörtert:

Gesprächsbedarf gab es im Zusammenhang mit den *Errichtungsanordnungen* für automatisierte personenbezogene Dateien für Ordnungsaufgaben nach dem Allgemeinen Gesetz zum Schutz der Öffentlichen Sicherheit und Ordnung in Berlin (ASOG). Nicht nur im Polizeibereich, sondern auch in den Bezirken gibt es viele Stellen, die solche Aufgaben wahrnehmen (z. B. Bau-, Gewerbe-, Veterinäraufsicht). Aufgrund der Ausführungsvorschriften zu § 49 ASOG (Dateirichtlinien) sind diese Stellen verpflichtet, für jede automatisierte Datei mit personenbezogenen Daten eine Errichtungsanordnung zu erlassen. Die einzelnen Angaben der im Zusammenhang mit den Ordnungsaufgaben erstellten Dateien werden auf einem Formular festgehalten und u. a. auch dem Berliner Beauftragten für Datenschutz und Informationsfreiheit gemeldet.

Viele Stellen waren der Meinung, dass sie die Errichtungsanordnung nicht auszufüllen brauchen, wenn sie schon eine Dateiregistermeldung nach altem Recht abgegeben haben. Auch eine Dateibeschreibung nach § 19 Abs. 2 Berliner Datenschutzgesetz (BlnDSG), die mit der Novellierung des Gesetzes im Jahre 2001 eingeführt wurde und an die Stelle der Dateiregistermeldung gesetzt worden war, ersetzt nicht die Errichtungsanordnung, da die Angaben nicht deckungsgleich sind.

Hinsichtlich des *Zugriffs von Mitarbeitern der bezirklichen Ordnungsämter auf Daten des Kraftverkehrsamtes* wird derzeit geprüft, ob zur Schaffung der rechtlichen Grundvoraussetzungen der Erlass einer Rechtsverordnung erforderlich ist. Derzeit darf nur die Polizei neben dem Kraftverkehrsamt auf die Daten zugreifen. Eine Stellungnahme der Senatsverwaltung für Inneres zu den rechtlichen Rahmenbedingungen steht noch aus.

Aufgrund des Urteils des Berliner Verwaltungsgerichts vom 10. August 2004 hinsichtlich der *Zuständigkeiten der Geschäftsstelle zur Koordinierung und Beratung bezirklicher IT-Verfahren (KoBIT)* bei personalvertretungsrechtlichen Beteiligungsverfahren zur Einführung von IT-Verfahren in den Bezirken erfolgte eine Abstimmung zwischen der Senatsverwaltung für Inneres, dem Hauptpersonalrat und der KoBIT statt. Im Ergebnis wurde festgehalten, dass die Senatsverwaltung für Inneres sich bereit erklärt hat, die Beteiligung für die bezirklichen Verfahren beim Hauptpersonalrat zentral durchzuführen, sofern es sich um ein Verfahren handelt, welches von mehr als einem Bezirk eingesetzt werden soll. Hier ergab sich die Frage, ob in solchen Fällen zur Verfahrensvereinfachung auch eine zentrale Beteiligung des Berliner Beauftragten für Datenschutz und Informationsfreiheit möglich ist.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist in jedem Fall von der für das Verfahren verantwortlichen Stelle nach § 24 Abs. 3 Satz 3 BlnDSG zu informieren. Gleichwohl sind die behördlichen Datenschutzbeauftragten aufgrund der unterschiedlichen IT-Umgebungen in den Bezirken auch dann immer in die Verfahren einzubeziehen, wenn die Unterrichtungspflichten und ggf. die Vorabkontrolle nach § 5 Abs. 3 Satz 2 BlnDSG von Seiten der KoBIT oder dem Pilotbezirk an einer Stelle durchgeführt wurden. Auf jeden Fall müssen ergänzend zu den zentralen Ergebnissen der Vorabkontrolle bezirksspezifische Anpassungen vorgenommen werden.

Erneut stand die Frage der Aufgabenabgrenzung zwischen dem behördlichen Datenschutzbeauftragten und anderen mit dem Datenschutz beauftragten Personen im Bezirksamt (u. a. Datenschutzbeauftragte im Sozialbereich, die auch nach Wegfall der Pflicht zu ihrer Bestellung nach Novellierung des SGB X weiter tätig sind, und Datenschutzbeauftragte in Schulen) zur Debatte.

Generell ist der behördliche Datenschutzbeauftragte für die Behörde oder sonstige öffentliche Stelle zuständig, für die er nach § 19 a BlnDSG bestellt wurde. Im Bereich der Schulen gehören Lehrer nicht zum Bezirksamt, also fällt der Datenschutz im Zusammenhang mit ihrer Tätigkeit nicht in den Verantwortungsbereich des jeweiligen bezirklichen Datenschutzbeauftragten. Die Schulen müssen einen eigenen Datenschutzbeauftragten bestellen. Dagegen ist für den Verwaltungsbereich der Schulen - hierzu zählen z. B. die Schulhausmeister und Schulsekretärinnen als Dienstkräfte des Bezirksamts - der Datenschutzbeauftragte des jeweiligen Bezirks zuständig.

Die formelle Verantwortlichkeit des bezirklichen Datenschutzbeauftragten muss aber nicht ausschließen, dass innerhalb des Bezirksamts weitere Kontaktpersonen zur Umsetzung des Datenschutzes für bestimmte Bereiche benannt werden, beispielsweise auf dem Gebiet des SGB X. Auch wenn die gesetzliche Pflicht zur Bestellung eines Datenschutzbeauftragten für den Sozialbereich nicht mehr besteht, so steht dem nichts entgegen, dennoch Mitarbeiter mit dieser Aufgabe für den Datenschutz in diesem senitiven und rechtlich komplexen Bereich zu betrauen.

Offene *Umlaufmappen* mit als „verschlossen“ und/oder „vertraulich“ gekennzeichneten Schriftstücken waren von Anfang an Dauerthema für den Berliner Beauftragten für Datenschutz und Informationsfreiheit, aber auch für die Datenschutzbeauftragten in den Bezirken. Sie stehen nach wie vor mit schöner Regelmäßigkeit vor dem Problem, dass Dokumente mit höchst vertraulichen Daten offen von Polizei, Staatsanwaltschaft und Amtsgerichten versandt und dann

ebenso innerhalb der Bezirksämter weitergeleitet werden. Es ist den Mitarbeitern der bezirklichen Poststellen kaum zu vermitteln, dass sie solche Dokumente in verschlossenen Mappen weitersenden müssen, wenn die sonst auf Vertraulichkeit erpichten Urheberbehörden dies nicht für nötig erachten. Der Polizeipräsident in Berlin und die Staatsanwaltschaft haben erneut in einem Rundschreiben an ihre Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Verpflichtungen, die sich aus § 5 BlnDSG auch für den Aktenverkehr ergeben, hingewiesen. Die Erfahrungen vieler bezirklicher Datenschutzbeauftragter zeigen jedoch, dass derartige gelegentlich wiederholte Maßnahmen leider nur für einen begrenzten Zeitraum Wirkung zeigen, weil sich nach einem gewissen Zeitablauf oder auch nach Personalwechsel immer wieder die gleichen Probleme zeigen.

Workshop der behördlichen Datenschutzbeauftragten der *Amtsgerichte*

Auch die behördlichen Datenschutzbeauftragten der Amtsgerichte finden mindestens zweimal im Jahr zu einem Erfahrungsaustausch, der die gemeinsamen Datenschutzprobleme in den Bereichen der Zivilgerichtsbarkeit behandelt.

Von besonderem Interesse war das Zwangsversteigerungsverfahren. Nicht nur Einzelpersonen, sondern verstärkt auch Firmen machen von ihrem *Einsichtsrecht nach § 42 Zwangsversteigerungsgesetz* (ZVG) Gebrauch und kopieren oder scannen immer häufiger die vorgelegten Unterlagen. In einigen Fällen erfolgt dies regelrecht geschäftsmäßig, indem von den Unterlagen und den daraus gezogenen Ergebnissen Broschüren erstellt und verkauft oder entsprechende Seiten ins Internet gestellt werden.

Insbesondere im Internet ist durch die ungehinderte Verbreitung und die über die Gebühr lange Verweildauer die Gefahr groß, dass ehemalige Schuldner, die längst schuldenfrei sind, immer noch als belastet dastehen und deshalb mitunter keine neuen Kredite bekommen oder um ihren Ruf fürchten müssen.

Veröffentlichungen von Zwangsversteigerungsterminen durch private Stellen im Internet enthalten regelmäßig personenbezogene Daten i. S. d. BDSG, und zwar auch dann, wenn nicht der Name des Eigentümers einer Immobilie, sondern nur die Anschrift des zu versteigernden Objekts angegeben wird. Es reicht die Benennung des Grundstücks aus, sich mit Hilfe weiterer Informationen, z. B. aus dem Grundbuch, Kenntnis über den Eigentümer zu verschaffen. Sowohl die Grundstücksanschrift als auch der Name des Eigentümers sind personenbezogene Daten.

Eine spezialgesetzliche Regelung für die Veröffentlichung von *Zwangsversteigerungsterminen*

durch private Stellen gibt es nicht. Lediglich für die Gerichte regelt § 40 Zwangsversteigerungsgesetz (ZVG), dass Informationen auch in anderer Weise als der Anheftung an die Gerichtstafel veröffentlicht werden dürfen. Dies ermächtigt jedenfalls die Gerichte dazu, eine eigene Internetseite einzurichten, um dort die Zwangsversteigerungstermine zu veröffentlichen.

Solange die gesetzliche Grundlage fehlt, wäre die Veröffentlichung von Zwangsversteigerungsterminen im Internet durch andere Stellen nur dann zulässig, wenn die betroffenen Personen darin einwilligen.

Mit der Einführung von *Hartz IV* und dem *Einsatz von sog. 1-Euro-Jobbern* gibt es auch bei den Amtsgerichten schwer wiegende Datenschutzkonflikte. So kommt in manchen Amtsgerichten dieser Personenkreis auch in Bereichen mit personenbezogenen Daten in Berührung, die als besonders sensibel gelten. Es wurde aus der Praxis berichtet, dass 1-Euro-Jobber in Aufgabengebiete eingebunden werden, die z. B. die Zwangsvollstreckung oder Nachlass- und Vormundschaftsangelegenheiten betreffen. Sie haben dort zum Teil Zugang zu allen Akten und sonstigen Unterlagen.

Nach unserer Auffassung dürfen erwerbsfähige Hilfsbedürftige nach § 16 Abs. 3 Satz 2 SGB II nicht in Bereichen eingesetzt werden, in denen sie mit personenbezogenen Daten in Berührung kommen. Dies gilt auch dann, wenn sie nach § 8 BlnDSG auf das Datengeheimnis verpflichtet wurden. Es steht außer Frage, dass diese Beschäftigten keine Dienstkräfte im Sinne des Gesetzes sind, da sie keine feste Anstellung bei den Gerichten haben.

Bestellung der Stellvertreter von behördlichen Datenschutzbeauftragten

> *Seit der gesetzlichen Verpflichtung im Zuge der Novellierung des Berliner Datenschutzgesetzes (BlnDSG) im Jahre 2001, einen Stellvertreter für den behördlichen Datenschutzbeauftragten zu bestellen, waren bis Mitte 2005 fünf Bezirksämter immer noch nicht dieser Verpflichtung nachgekommen. Wir haben diese Bezirksämter angeschrieben und nunmehr mit einer Fristsetzung dazu aufgefordert, dem Gesetz Folge zu leisten.*

Zwei Bezirksämter meldeten sich daraufhin umgehend und teilten uns die Bestellung unter Benennung der Stellvertreter mit. Ein weiteres Bezirksamt bat um Fristverlängerung, da die Gespräche mit geeigneten Mitarbeitern/innen noch nicht endgültig abgeschlossen waren.

Die Bezirksbürgermeisterin von Charlottenburg-Wilmersdorf teilte uns mit, dass es eine

Bestellung aufgrund der immer knapper werdenden personellen Ressourcen in den Bezirken auch in absehbarer Zeit in ihrem Bezirk nicht geben wird. Man wolle jedoch die Regelung treffen, dass für die Zeiträume, in denen der hauptamtliche Datenschutzbeauftragte abwesend ist, ein kompetenter Ansprechpartner im bezirklichen Rechtsamt zur Verfügung steht.

Wir wiesen das Bezirksamt auf die gesetzliche Forderung hin und betonten, dass die Pflicht zur Bestellung nicht unter dem Vorbehalt der verfügbaren finanziellen und personellen Möglichkeiten steht. Die formale Umsetzung dieser Verpflichtung, die mit dem o. g. Ansprechpartner, der vor der Bezirksfusion schon bezirklicher Datenschutzbeauftragter war, ohne weiteres möglich wäre, ist notwendig, damit dem Stellvertreter - zumindest im Vertretungsfall - auch die gleichen Kompetenzen und der Schutz der Unabhängigkeit gewährt werden, wie sie dem behördlichen Datenschutzbeauftragten durch das Gesetz zustehen. Der Bezirk Charlottenburg-Wilmersdorf hat die von uns gesetzte Frist verstreichen lassen und bisher keinen Stellvertreter des behördlichen Datenschutzbeauftragten benannt.

Der Bezirksbürgermeister von Neukölln verband die Pflicht zur Bestellung eines Stellvertreters des bezirklichen Datenschutzbeauftragten damit, dass er bis dahin von uns nicht explizit aufgefordert worden war. Dies ist zwar richtig, das Thema war aber regelmäßig Gegenstand der Gesprächskreise mit den bezirklichen Datenschutzbeauftragten, zu denen auch die Datenschutzbeauftragte des Bezirksamtes Neuköllns gehört. Wir erinnerten daran, dass gesetzliche Anforderungen nicht erst dann zu erfüllen sind, wenn man von anderer Seite daran erinnert wird. Im Übrigen sind die gesetzlichen Vorgaben unabhängig von haushaltsrechtlichen oder personalwirtschaftlichen Abwägungen zu erfüllen. Für die Bestellung des Stellvertreters setzten wir eine Frist, die erfreulicherweise genutzt worden ist.

Datenschutz bei kleinen Unternehmen

> *Eine geplante Änderung des Bundesdatenschutzgesetzes (BDSG) hat für Aufmerksamkeit gesorgt. Bei der entsprechenden Gesetzesinitiative der Länder Niedersachsen und Hessen[107] ging es im Kern um die Neuformulierung der §§ 4 d Abs. 3 und 4 f Abs.1 Satz 1 BDSG. Die dort verankerte Begrenzung der erforderlichen Mitarbeiterzahl für die Meldepflicht von Datenverarbeitungsverfahren bzw. die Bestellpflicht für einen betrieblichen Datenschutzbeauftragten soll von 5 auf 19 Arbeitnehmer heraufgesetzt werden.*

Dem mit der Initiative geplanten *Bürokratieabbau* stehen Stimmen gegenüber, die vor der Realisierung dieses Vorhabens warnen, da mit der geplanten Heraufsetzung eine große Anzahl

107 BR-Drs. 599/05

von Kleinunternehmen der Erfassung durch die vorgegebenen Aufsichtsstrukturen entzogen werden.

Mit § 4 d BDSG hat der Gesetzgeber in Umsetzung von Artikel 18 EG-Datenschutzrichtlinie den Versuch unternommen, eine erhöhte Transparenz der Datenverarbeitung zu erreichen und eine materielle Zulässigkeitskontrolle sensitiver Verarbeitungen festzulegen. Eine Begrenzung der Mitarbeiterzahl für die Bestell- und Meldepflicht wurde nicht in der Richtlinie vorgeschrieben; diese ist erst mit der Novellierung des BDSG im Jahr 2001 auf fünf Arbeitnehmer festgelegt worden. Seitdem hat z. B. die zunehmende Automation des Zahlungswesens durch den täglichen Einsatz von EC- und Kreditkarten im Einzelhandel, bei Warenhäusern oder Tankstellen, oder aber die Nutzung von Computertechnik in Arztpraxen, Apotheken, Rechtsanwalts- und Steuerberaterkanzleien dazu geführt, dass immer mehr Klein- und Kleinstbetriebe aufgrund der Vorschriften des BDSG verpflichtet werden, einen betrieblichen Datenschutzbeauftragten zu bestellen.

Die Initiatoren der Gesetzesänderung argumentieren mit der Absicht, einen Beitrag zur Entbürokratisierung und Senkung der Kosten in den Betrieben leisten zu wollen. Die komplizierte Gesetzesregelung hat gerade bei den kleinen Betrieben und Kleinstunternehmen oft zu Unklarheiten und Missverständnissen bei der Beachtung der Meldepflicht und der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten geführt.

Dagegen spricht, dass gerade bei kleinen Unternehmen erhebliche Datenschutzdefizite festzustellen sind, denn auch sie verfügen über erhebliche Risikopotenziale für Eingriffe in die Datenschutzrechte der Bürger. Mit der Heraufsetzung der erforderlichen Mitarbeiterzahl würden unzählige dieser kleinen Unternehmen durch das Raster fallen und die zurzeit für diese Unternehmen bestehende Aufsicht, die sowohl durch den betrieblichen Datenschutz-beauftragten oder aber durch die Aufsichtsbehörde ausgeübt wird, würde künftig mit dem Wegfall des Bestellungserfordernisses bzw. der Meldepflicht ersatzlos entfallen.

Anzumerken ist, dass die geplante Begrenzung z. B. nicht für *Arztpraxen* oder *Apotheken* gelten würde, da durch die Verarbeitung sensitiver Gesundheitsdaten i. S. v. § 3 Abs. 9 BDSG eine Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten nach § 4 f Abs. 1 Satz 6 i. V. m. § 4 d Abs. 5 Nr. 1 BDSG in jedem Fall bestehen bleibt, nämlich dann, wenn eine Vorabkontrolle durchzuführen ist.

Externe Datenschutzbeauftragte* für *Arztpraxen* und *Apotheken

Viele Arztpraxen und auch Apotheken können mitunter wegen zu geringer Mitarbeiterzahl keinen betrieblichen Datenschutzbeauftragten bestellen. Das Bundesdatenschutzgesetz (BDSG) erlaubt jedoch ausdrücklich den Einsatz von externen Datenschutzbeauftragten. Die Externen können dabei sowohl für nur eine Stelle als auch für mehrere Stellen tätig werden. Idealerweise sollte der Datenschutzbeauftragte jedoch aus dem Kreis der Mitarbeiter dieser Stellen kommen.

Problematisiert wurde in diesem Zusammenhang die Frage, ob der externe Datenschutzbeauftragte bei Stellen, die einem Berufsgeheimnis - hier dem Arzt- bzw. Apothekergeheimnis - unterliegen, die gleichen Befugnisse haben soll wie ein interner, betrieblicher Datenschutzbeauftragter. Während die einen sagen, der externe Datenschutzbeauftragte hat die gleichen Aufgaben und Kompetenzen wie ein interner Datenschutzbeauftragter, behaupten andere hingegen, der Externe dürfe zwar abstrakte Rechtsfragen bearbeiten, dabei aber nicht auf die besonders sensiblen Patientendaten zugreifen. Gerade vor dem Hintergrund der geplanten Einführung der elektronischen Gesundheitskarte und des elektronischen Rezeptes wird die Brisanz dieses Problems deutlich.

Keine rechtlichen Einwände bestehen, wenn es sich bei dem betrieblichen Datenschutzbeauftragten (bDSB) um einen Mitarbeiter der verantwortlichen Stelle handelt. Ein interner Datenschutzbeauftragter kennt die Betriebsabläufe in der Apotheke oder Arztpraxis und weiß, welche personenbezogenen Daten wann, wo und wie verarbeitet werden. In diesem Fall unterliegt der betriebliche Datenschutzbeauftragte nicht in seiner Eigenschaft als Datenschutzbeauftragter, sondern nur in seiner Eigenschaft als Angestellter der Weisungsbefugnis des jeweiligen Arztes oder Apothekers; seine Unabhängigkeit als Datenschutzbeauftragter bliebe gewahrt. Als Angestellter ist er Hilfskraft des Arztes oder des Apothekers, dem im Rahmen der Erforderlichkeit Berufsgeheimnisse offenbart werden dürfen; auch er unterliegt der Schweigepflicht.

Ein externer Datenschutzbeauftragter wird aufgrund der größeren Erfahrung professioneller agieren können als ein interner Mitarbeiter. Er kann sich den Datenschutzproblemen im Unternehmen intensiver und unvoreingenommener widmen als ein interner Datenschutzbeauftragter, der in der Regel noch andere Aufgaben zu bewältigen hat. Es darf jedoch nicht übersehen werden, dass die Unabhängigkeit externer Beauftragter stärker eingeschränkt ist als die von internen Mitarbeitern, weil der Abberufungsschutz nach § 4 f Abs. 3 Satz 4 BDSG (nur bei entsprechender Anwendung von § 626 BGB – außerordentliche Kündigung) bei freiberuflicher Beauftragung nicht gegeben ist.

Diskutiert wurde auch die Konstellation, nach der zwei Datenschutzbeauftragte - eine externe Kraft und ein interner Mitarbeiter - gleichzeitig den Datenschutz betreuen könnten; dabei soll der externe Beauftragte die Hauptarbeit leisten, der interne nur dann tätig werden, wenn Patientendaten ins Spiel kommen. Dieser Vorschlag wird bei kleinen Stellen in der Regel aus organisatorischen, personellen oder letztlich auch aus Kostengründen scheitern.

Im Düsseldorfer Kreis, der Konferenz der Obersten Aufsichtsbehörden für den Datenschutz, hat man sich darauf verständigt, dass die Bestellung eines externen Datenschutzbeauftragten bei Berufsgeheimnisträgern zulässig sei. Unterschiedliche Auffassungen bestehen hinsichtlich der Frage, ob sich seine Kontrollkompetenz auch auf die dem Berufsgeheimnis unterliegenden Daten bezieht. Die Mehrheit des Düsseldorfer Kreises vertritt die Auffassung, dass sich die Kontrollkompetenz auf alle Daten bezieht, die von dem Berufsgeheimnisträger erhoben, verarbeitet oder genutzt werden.

4.9.2 Kontrolle des Verfahrens SpDI32

Im Jahresbericht 2001[108] erwähnten wir das in der Planung befindliche IT-Verfahren für die Aufgabenerfüllung der Sozialpsychiatrischen Dienste (SpDI32). Wir nahmen dies seinerzeit zum Anlass, auf die besonders schutzbedürftigen Daten von psychisch kranken Menschen und gleichzeitig auf die strikte Beachtung der damals neuen Vorschriften zu den technisch-organisatorischen Maßnahmen des Datenschutzes hinzuweisen.

Nachdem das Verfahren nunmehr in mehreren Bezirken eingeführt wurde, haben wir eine datenschutzrechtliche Kontrolle des Verfahrens beim Sozialpsychiatrischen Dienst des Bezirksamtes Steglitz-Zehlendorf (örtlicher Bereich Steglitz) durchgeführt. Das Bezirksamt ist Pilotbezirksamt für das Verfahren und hat somit die Verfahrensverantwortung übernommen. Gegenstände der Kontrolle waren die Umsetzung der Vorschriften des Sozialgesetzbuchs X (SGB X) für das IT-Verfahren SpDI32 und die technisch-organisatorischen Maßnahmen zum Datenschutz nach der Anlage zu § 78 a SGB X.

Die Ergebnisse der Kontrolle lassen sich zum Teil auf andere Bezirke übertragen, soweit sie sich ausschließlich auf das Verfahren beziehen. Fragestellungen zu technisch-organisatorischen Aspekten lassen sich dagegen nicht übertragen, weil jeder Bezirk eine eigene individuelle technische Infrastruktur betreibt.

---

108 vgl. 2.2

Die Aufgaben der Sozialpsychiatrischen Dienste (SozPsychD) bestehen in der Betreuung psychisch kranker Personen, dazu gehören auch Suchtkranke, soweit sie nicht von niedergelassenen Ärzten betreut werden. Für diese Personen wird die Hauspflege in Zusammenarbeit mit Sozialstationen koordiniert und ggf. eine Unterbringung veranlasst. Es werden Gutachten für Kostenträger – insbesondere das Sozialamt – erstellt, um die Kostenübernahme zu klären. Ferner werden Gutachten für Gerichte erstellt.

Der SozPsychD wird in der Regel durch telefonische oder schriftliche Hinweise aus der Nachbarschaft oder dem sozialen, auch familiären Umfeld auf Hilfebedürftige aufmerksam. Seltener ist, dass ein Betroffener selbst vorspricht, dann meist auf Drängen der Familie. Ein Sozialarbeiter nimmt die Meldung auf, veranlasst das sofort Notwendige und bringt dann den Fall in sein Team ein. Ein Arzt erstellt die Diagnose und entscheidet, was weiter geschehen soll.

Die Weitergabe von personenbezogenen Daten aus SpDI32 erfolgt ausschließlich bei Anfragen im Einzelfall oder als Gutachten. Die Datenweitergabe an die Senatsverwaltung für Gesundheit, Soziales und Umweltschutz zum Zwecke der Gesundheitsberichterstattung erfolgt ausschließlich mit aggregierten Daten, die keinen Personenbezug mehr aufweisen.

Für die Datenübertragung zwischen dem zentralen Computer (Server) und den Arbeitsplatz-computern (Clients) wurde eine Datenverschlüsselung integriert. Dies verhindert, dass bei Angriffen auf die Datenleitung Daten im Klartext ausgelesen werden können. Der Zugriff wurde für die berechtigten Nutzer sehr differenziert geregelt, so dass sie ausschließlich im Rahmen ihrer Befugnis auf die sehr sensitiven Daten zugreifen können. Die Datensicherung wird regelmäßig erstellt und an einem sicheren Ort aufbewahrt, so dass nach einem Schadensfall ohne erheblichen Mehraufwand eine Rücksicherung des vorhandenen Datenbestandes möglich ist.

Allerdings lagen eine Risikoanalyse und ein darauf aufbauendes Sicherheitskonzept nicht vor. Das ist ein Verstoß gegen § 5 Abs. 3 Berliner Datenschutzgesetz, welches gerade diese fordert, um die sichere Verarbeitung personenbezogener Daten zu gewährleisten. Nur bei Beachtung dieser Vorschrift ist für die Verantwortungsträger im Bezirksamt nachvollziehbar, ob die getroffenen Maßnahmen gegen bestehende Risiken angemessen sind und ob Risiken bestehen, gegen die keine hinreichenden Maßnahmen ergriffen worden sind. Solche Konzepte sind sowohl für das Verfahren als auch für die IT-Infrastruktur des Bezirksamtes zu erstellen. Diese lagen jedoch nur zum Teil oder in überarbeitungsbedürftiger Version vor. Das Bezirksamt hat zugesagt, hier Abhilfe schaffen zu wollen.

Ein weiterer Kritikpunkt betraf die Sperrung von Daten. Obwohl das Verfahren Daten von

Betroffenen für einen langen Zeitraum speichert, wurde versäumt, technische Möglichkeiten für die Sperrung von Daten zu schaffen, die z. B. nach dem Tod eines Klienten genutzt werden müssen, da die Daten für die Bearbeitung nicht mehr benötigt werden. Wir haben vorgeschlagen, eine Sperre sechs Monate nach dem Tod eines Klienten einsetzen zu lassen, da bis zu diesem Zeitpunkt die Daten im Zusammenhang mit Nachlassregelungen o. Ä. noch benötigt werden. Auf gesperrte Daten darf nur unter der besonderen Verantwortung der Behördenleitung zugegriffen werden. Unsere Anregung wurde positiv aufgenommen und soll in einer zukünftigen Programmversion ergänzt werden. Bis zu einer entsprechenden softwareseitigen Umsetzung werden organisatorische Maßnahmen ergriffen.

Das Verfahren beinhaltet eine Schnittstelle zu einem externen Textverarbeitungsprogramm. Hierdurch ist ein Export sämtlicher in SpDI32 gespeicherten Daten in entsprechende Dokumente außerhalb des geschützten Verfahrens möglich. Dies setzt allerdings Dokumentenvorlagen voraus, die nur von besonders berechtigten Nutzern erstellt werden können. Die Speicherung der Dokumente ist jedoch nicht im Verfahren vorgesehen, sondern erfolgt außerhalb des Schutz bietenden Verfahrens. Einerseits sind die in der SpDI32-Datenbank gespeicherten sensitiven personenbezogenen Daten gegen unbefugte Kenntnisnahme zusätzlich durch Verschlüsselung geschützt, andererseits entfällt dieser Schutz mit dem Transfer solcher Daten in Dokumente. Die Übertragung der besonders schutzbedürftigen personenbezogenen Daten erfolgt somit unverschlüsselt zwischen den Arbeitsplatzcomputern und dem Server. Sollten auf diesem Übertragungsweg Daten abgegriffen werden, so wären diese im Klartext lesbar. Gleiches gilt bei unbefugten Zugriffen auf den Server.

Unserer Empfehlung, dass Schreiben mit personenbezogenen Daten aus SpDI32 in die Sicherheitsdomäne von SpDI32 einbezogen und damit ebenfalls verschlüsselt gespeichert und übertragen werden, wurde bisher nicht gefolgt. Eine abschließende Bewertung kann jedoch erst dann erfolgen, wenn das schon oben erwähnte Sicherheitskonzept für das Behördennetz vorliegt, in dem das genannte Risiko eingehend gewürdigt wird. Dann kann auch abschließend beurteilt werden, ob die ergriffenen Maßnahmen gegen ein Ausspähen dieser in Klartext vorliegenden Daten auf dem Übertragungsweg und auf dem Server wirksam greifen.

Die Passwortregelungen für die Anmeldung an das Verfahren SpDI32 wurden vorbildlich umgesetzt. Sie beinhalten z. B. eine Mindestpasswortlänge oder einen regelmäßigen Passwortwechsel. Vergessen wurde jedoch, dass die Systempasswörter an einem sicheren Ort hinterlegt werden sollten, damit auch in Notfallsituationen – z. B. bei Ausfall des Systemadministrators – die Verfügbarkeit des Systems sichergestellt werden kann.

Die Vernichtung von Akten wird nach nachvollziehbaren Aufbewahrungsfristen von einem

Vernichtungsunternehmen durchgeführt. Ein Konzept für die Löschung der Daten im System lag jedoch nicht vor. Es wurde in der Zwischenzeit erarbeitet.

Die Abarbeitung der vorgefundenen Mängel erfolgt in einem vertretbaren Zeitrahmen. Schon unmittelbar nach der Kontrolle wurde uns eine Dienstanweisung zugesandt, die Regelungen zur Papiervernichtung und zum Löschkonzept beinhaltet.

4.9.3 Datenschutz im IT-Verfahren IPV

> *Die Personalverwaltung des Landes Berlin wird elektronisch durch das Verfahren IPV (Integrierte Personal Verwaltung) unterstützt. Mit IPV soll die Personalverwaltung vereinfacht werden, indem verschiedene Funktionen von der Bearbeitung von Urlaubs- oder Teilzeitanträgen bis zu den Lohn- und Gehaltsbuchungen einzelner Stellen zusammengefasst werden. Mittlerweile wurden Funktionen der Büroleitung, der Personalwirtschaftsstellen, der Personalaktenführung hinzugefügt.*

Herzstück dieses Verfahrens ist die integrierte, von Branchen unabhängige Standardsoftware R/3 des deutschen Softwarehauses SAP. Über die Entwicklung haben wir kontinuierlich berichtet[109]. Für die Realisierung von IPV wird aus den vielen Modulen, die R/3 zur Abbildung von betriebswirtschaftlichen Anwendungsgebieten (z. B. Rechnungswesen, Logistik oder Personalwirtschaft) bereitstellt, lediglich das Modul HR (Human Resources) verwendet. Die Nutzungsbedingungen erlauben die Nutzung weiterer R/3-Module, so dass auch andere Fachverfahren auf dieser Plattform realisiert werden sollen. Ein Beispiel ist die Teilnehmerverwaltung für Fortbildungen bei der Justizverwaltung. Die Fachverfahren nutzen weitere Module der Standardsoftware R/3, die zurzeit nicht durch IPV genutzt werden. Obwohl eine formale Trennung der Verfahren beispielsweise hinsichtlich des Verfahrensbetreibers vorliegt, so sind sie dennoch aus technischer Sicht Bestandteil von IPV. Dies hat zur Folge, dass alle diese Verfahren an die Sicherheitsvorgaben von IPV gebunden sind. Im Wesentlichen ist ein Zugriffsmodell zu erstellen, das in SAP-R/3 über das Berechtigungskonzept umzusetzen ist. Es sind bereits weitere Verfahren in Planung, deren Umsetzung wir mit Interesse begleiten werden.

Wie die meisten Softwareprodukte unterliegt auch das SAP-R/3-System einem fortlaufenden Wandel und Erneuerungsprozess. Diesem Umstand wird in Form von sog. Updates Rechnung getragen. Bei R/3 werden kleine Änderungen an der Software durch sog. Patches vorgenommen. Größere Veränderungen erfordern einen sog. Release-Wechsel. Mit dem

109 JB 1998, 4.8.1 und JB 1999, 4.4.1

Release-Wechsel von Version 4.5 auf 4.7 erfolgte allerdings eine Verschlechterung der IT-Sicherheit mit daraus resultierendem erhöhtem Betriebsrisiko, indem SAP ein Sicherheitsmodul ersatzlos aus der Software R/3 entfernt hat. Durch das Weglassen dieses Sicherheitsmoduls ist es möglich, sensitive personenbezogene Daten im erweiterten Umfang über die Exportfunktion aus der sicheren IPV-Umgebung herauszuziehen, z. B. zur Erstellung von Serienbriefen. Gründe für diese Änderung waren nicht in Erfahrung zu bringen.

Über diese Entwicklung wurden wir durch den Verfahrensbetreiber, das Landesverwaltungsamt, informiert, der für diesen Fall um Beratung bat. Das Ergebnis der Beratung fand unmittelbar Eingang in das zum Ende des Jahres fertig gestellte neue Sicherheitskonzept des Verfahrens. Das Konzept befasst sich unter anderem mit den wesentlichen Änderungen und Erweiterungen des Verfahrens. Weiterführende Erkenntnisse konnten wir aufgrund des erst kürzlich erfolgten Zugangs noch nicht gewinnen.

4.9.4 Sicherheit in lokalen *Funknetzen* (WLAN)

> *Bereits im Jahresbericht 2001[110] machten wir auf Datenschutzprobleme bei Wireless local area Networks (WLAN) aufmerksam. Diese Technologie macht den Betrieb lokaler Rechnernetze von baulichen Gegebenheiten weitgehend unabhängig, es kann auf die Verlegung von vielen Kabeln verzichtet werden. Die Flexibilität für den Standort der angeschlossenen Rechner, insbesondere von mobilen Rechnern, innerhalb der Reichweite der WLANs spricht ebenfalls in vielen Fällen für diese Technologie. Den Vorteilen für eine flexible Arbeitsorganisation, für den Geldbeutel des Betreibers und in vielen Fällen auch den Denkmalschutz stehen jedoch Risiken für die Vertraulichkeit der übertragenen Daten und für die Integrität der Daten und Verfahren gegenüber.*

Mit dem Einsatz dieser Technik ist es möglich, dass Anwender, die über einen Rechner mit einer entsprechenden Funknetzwerkkarte verfügen und sich im Empfangsbereich eines Netzes aufhalten, diesen automatisch in das Netzwerk integrieren könnten. Dieser Vorgang funktioniert ohne Benutzereingriff voll automatisiert und lässt sich mit dem Anschluss eines Rechners an die bestehende Datenverkabelung vergleichen. Denn Funkwellen kennen keine räumlichen Barrieren für die Versendung und den Empfang der Signale. So kann der Parkplatz vor der Firma schon ein sehr guter Angriffspunkt sein. Zum unbefugten Eindringen in lokale Netze ist bei normaler Verkabelung immerhin der physische Zugang zum LAN-Kabel notwendig, bei Funknetzen reicht bei unzureichenden Sicherheitseinstellungen eine Funknetzwerkkarte für das Notebook.

---

110 vgl. 4.8.3

Seit wir im Jahresbericht 2004[111] das Thema erneut aufgegriffen und über die Aktivitäten des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder berichtet haben, sind Fortschritte bei der Entwicklung der IT-Sicherheit bei WLANs zu verzeichnen.

Neben den Standardanforderungen wie dem Einsatz von Firewalls an den Schnittstellen zu Internet und Intranet, Verhinderung der automatischen Zuteilung von IP-Adressen, verschlüsselter Datenübertragung, gesichteter Authentifikation, Intrusion Detection System, Abwehr von Schadprogrammen sowie den organisatorischen und personellen Maßnahmen zur Verbesserung der Sicherheit beim Einsatz von WLANs kommen jetzt Verbesserungen zur Geltung, die in der Anpassung der Standardisierung an höhere Sicherheitsanforderungen begründet liegen.

Durch den neuen Standard 802.11 i mit dem Wi-Fi Protected Access (WPA)-Verfahren wurden wesentliche Verbesserungen für die Sicherheit von WLANs eingeführt. Hierbei zertifiziert die Wi-Fi Alliance neue Implementierungen für mehr Sicherheit und bildet eine Teilmenge des WEP-Nachfolgestandards. Die neue WPA-Verschlüsselung sollte ausschließlich genutzt werden, denn im Gegensatz zum alten WEP-Verfahren hat sie sich bisher als hinreichend sicher erwiesen.

Inzwischen wurde die Orientierungshilfe „Datenschutz in drahtlosen Netzen“ vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgeschlossen und steht Interessierten im Internet zur Verfügung (http://www.datenschutz.mvnet.de/informat/wlan/oh_wlan.html).

4.9.5 Datensicherheit bei digitalen *Kopiersystemen*

In den letzten Jahren ist der Wandel von analogen zu digitalen Kopiersystemen vollzogen worden. Wesentliche Vorteile sind die besseren Laufeigenschaften durch weniger mechanische Teile und die bessere Druckqualität durch Lasertechnologie. Dadurch wird auch die Wirtschaftlichkeit dieser Produkte noch effektiver. Weitere Vorteile sind die Optionen, diese zu Netzwerkdruckern, Scannern oder sogar zu Faxgeräten aufzurüsten. In Sekretariaten sind multifunktionale Kopiersysteme (Kopierer, *Fax, Drucker* und *Scanner* in einer Einheit) kaum noch wegzudenken. Diese leistungsfähigen Geräte sind heutzutage im Netzwerk als zentrale Büro- oder Abteilungsdrucker vielseitiger und wirtschaftlicher als herkömmliche Drucker.

111 vgl. 3.5

Da diese Multifunktionssysteme auch ins Unternehmensnetz integriert werden und sogar Verbindung zum Internet aufnehmen können, benötigen sie ähnliche Sicherheitsvorkehrungen wie PCs oder Server. Vor allem durch die Netzwerkfähigkeit können die Geräte zu einem Sicherheitsrisiko im Unternehmen werden. Das zentrale Problem ist hierbei die Datensicherheit solcher Systeme.

Datenschutzrisiken könnten beispielsweise bei der Rückgabe bzw. Entsorgung gemieteter Geräte an den Hersteller entstehen. Einige Hersteller reagieren darauf mit verschiedenen Ansätzen: Sie statten ihre Produkte mit Funktionen zur *Festplattenverschlüsselung* aus. Demnach sollen die Daten verschlüsselt abgelegt und daher von Außenstehenden nicht zu entschlüsseln sein. Die Firma Sharp Electronics wirbt mit ihrem Sicherheits-Feature *Data Security Kit* für erhöhte Datensicherheit, wobei die vollständige Löschung aller Daten durch Überschreiben mit Zufallszahlen erfolgen soll.

Alle Kopien und gedruckten Dokumente werden im internen (Zwischen-)Speicher eines digitalen Kopiersystems abgelegt. Unklar ist hingegen die Art und Dauer der Speicherung. Die Annahme, dass die Daten im internen (Zwischen-)Speicher abgelegt und je nach Größe eines weiteren zu druckenden Dokuments bzw. je nach Bedarf beliebig überschrieben werden, konnte bisher nicht eindeutig bestätigt werden und wäre aus Sicht des Datenschutzes auch unbefriedigend.

Aus diesem Grund wurden Erfahrungen mit dieser Problemstellung im Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten ausgetauscht. Es wurde die einhellige Meinung geäußert, dass an digitale Kopiersysteme die gleichen Anforderungen gestellt werden sollten wie an sonstige EDV- oder TK-Komponenten (PC, Server, Faxgeräte etc.).

Speziell sollte Folgendes beachtet werden:

- Digitale Kopier- und Drucksysteme sind Geräte, die im Rahmen der automatisierten Datenverarbeitung eingesetzt werden. Ihr Einsatz ist daher bei den nach § 5 Abs. 3 Berliner Datenschutzgesetz erforderlichen Risikoanalysen und Sicherheitskonzepten einzubeziehen. Neben der schon immer bei Kopierern und Druckern notwendigen Sicherung der Kopien und Ausdrucken vor unbefugter Beseitigung oder Kenntnisnahme ist bei den mit Speichern ausgestatteten digitalen Systemen zu verhindern, dass die gespeicherten Daten von Unbefugten gelesen, verändert oder gelöscht werden können.

- Normalerweise ist nicht festgelegt, wer zum Kopieren befugt ist. Vielmehr darf jeder im Rahmen seiner Aufgabenerfüllung kopieren, so dass individuelle Berechtigungsprofile keinen Sinn machen. Deshalb dürfen beim normalen Kopieren keine Datenspeicherungen vorgenommen werden, die ohne einen erheblichen technischen Aufwand ausgelesen werden können. Die fortdauernde Speicherung darf nur im Einzelfall bewusst ausgelöst werden können, weil die Daten für spätere Vorgänge wiederverwendet werden sollen.

- Für eine differenzierte Regelung des Zugriffs auf gespeicherte Dokumente muss das System individuelle Lese- und Löschungsrechte auf einzelne Dokumente ermöglichen und mit einem Authentisierungsverfahren (z. B. Kennung und Passwort, ID-Karte) die Berechtigungsprüfung ermöglichen.

- Der Systembetreiber muss alle gespeicherten Informationen datenschutzgerecht löschen können. Eine Systemverwaltung muss in der Lage sein, alle Dokumente lesen und löschen zu können, bei vernetzten Systemen auch von abgesetzten Arbeitsplätzen.

5. Telekommunikation und Medien

5.1 Telekommunikationsdienste

Der drohende Dammbruch - Vorratsspeicherung von Telefon- und Internetdaten

Entwürfe zur Einführung einer Vorratsspeicherung von Verkehrsdaten werden in Brüssel seit langem diskutiert. Hierbei geht es im Kern um die Speicherung sämtlicher Verbindungs- und Standortdaten, die bei der Abwicklung von Diensten der elektronischen Kommunikation anfallen. Konkrete Formen nahmen die Diskussionen nach den Terroranschlägen in Madrid im Frühjahr 2004 an. Der EU-Rat legte den Vorschlag für einen *Rahmenbeschluss* zur *Vorratsdatenspeicherung* vor[112]. Damit hatten wir uns bereits in unserem letzten Jahresbericht befasst[113]. Kritiker – unter anderem das Europäische Parlament – hatten neben inhaltlichen Vorbehalten auch geltend gemacht, dass der Ministerrat keine ausreichende gesetzliche Befugnis habe, um derart weit reichende Regelungen ohne Beteiligung des Parlaments zu erlassen.

Seit den Anschlägen in London im Juli 2005 unterstützt auch die EU-Kommission die Pläne mit einem parallelen Gesetzgebungsverfahren und hatte im September 2005 einen ersten offiziellen Entwurf für eine *Richtlinie* über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, vorgelegt[114]. Die Kommission erhofft sich dadurch bessere Möglichkeiten zur Prävention, Aufklärung und Verfolgung schwerer Straftaten, vor allem im Bereich des Terrorismus und der organisierten Kriminalität. Es sei ein Harmonisierungsbedarf innerhalb der EU gegeben, da einzelne Mitgliedstaaten divergierende nationale Maßnahmen zur Vorratsdatenspeicherung verabschiedet hätten oder dies planen würden.

Dem Vorschlag zufolge sollten Telekommunikationsanbieter verpflichtet werden, Verbindungsdaten, die beim Telefonieren im Fest- oder Mobilfunknetz anfallen, für ein Jahr zu speichern, auch wenn sie für betriebliche Zwecke, z. B. zur Abrechnung, nicht mehr benötigt werden. Für Daten aus den Bereichen Internetzugang, E-Mail und Internet-Telefonie war eine Speicherfrist von sechs Monaten vorgesehen. Die Pflicht zur Speicherung bezieht sich dabei

112 vgl. Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, und Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für Ermittlung, Aufklärung und Verfolgung bei Straftaten, einschließlich Terrorismus, in der Fassung v. 29. Juni 2005

113 JB 2004, 5.1

114 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG v. Vorschlag für eine Richtlinie des Europ.

auf sämtliche Daten, welche die Quelle, das Ziel, die Art und im Mobilfunk den Ort einer Kommunikation bestimmen. Die als Anlage zu dem Entwurf vorgesehene Liste mit den vorzuhaltenden Daten-typen umfasst unter anderem die Rufnummer des anrufenden oder angerufenen Anschlusses, den Namen und die Anschrift des Teilnehmers bzw. registrierten Nutzers, die dynamische oder statische IP-Adresse, die zugewiesene Benutzerkennung, den Beginn und das Ende des Kommunikationsvorgangs (z. B. An- und Abmeldung beim Internet-Zugangsdienst), die in Anspruch genommenen Dienste (z. B. Sprachtelefonie, Telefax, SMS, MMS), die internationale Mobilfunkteilnehmerkennung (IMSI), die internationale Mobilfunkgerätekennung (IMEI) und die Standortkennung (Cell-ID) im Mobilfunk. Diese Daten sollen den nationalen Sicherheits-behörden unter bestimmten Voraussetzungen zu Zwecken der Strafverfolgung zur Verfügung stehen.

Die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* hat in einer Entschließung an die Bundesregierung, den Bundestag und das Europäsche Parlament appelliert, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen[115]. Die Annahme des Richtlinienvorschlags und ihre Umsetzung in nationales Recht würden einen Dammbruch zu Lasten des Datenschutzes unverdächtiger Bürger bedeuten. Bei entsprechender Auswertung der zu speichernden Informationen ließen sich umfassende *Kommunikations- und Bewegungsprofile* für einen Großteil der Bevölkerung erstellen. Sowohl das grundgesetzlich geschützte Fernmeldege-heimnis als auch der durch die *Europäische Menschenrechtskonvention* garantierte Schutz der Privatsphäre drohten unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden. Die Datenschutzkonferenz weist weiter darauf hin, dass alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) bisher nicht ernsthaft erwogen worden seien. Mit einem solchen „*Quick freeze“-Verfahren* könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen. Schließlich warnt die Konferenz vor einer Ausweitung der Vorratsspeicherung auch auf Inhaltsdaten. Schon jetzt sei die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen.

Die Einführung einer Verpflichtung zur anlassunabhängigen Speicherung aller Verkehrsdaten der Telefon- und Internetkommunikation würde dazu führen, dass auch unverdächtige Nutzer dieser Netze unter Generalverdacht gestellt würden.

Die *Art. 29-Datenschutzgruppe* hat sich ebenfalls kritisch gegenüber dem Richtlinienvorschlag

115 Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 27./28. Oktober 2005 „Keine Vorratsdatenspeicherung in der Telekommunikation“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 14

geäußert[116]. Sie verkennt nicht das Risiko, das terroristische Bedrohungen für eine demokratische Gesellschaft bedeuten. Allerdings bezweifelt sie, dass die Begründungen für eine generelle obligatorische Vorratsdatenspeicherung überzeugend sind. Sollte es gleichwohl zu einer verpflichtenden Vorratsdatenspeicherung kommen, müsse deren Zweck klar definiert sein. Es müsse ein Zusammenhang mit der Bekämpfung des Terrorismus und des organisierten Verbrechens bestehen. Die Speicherfrist sollte so kurz wie möglich und zugleich eine für alle Mitgliedstaaten verbindliche Höchstgrenze sein. Den Mitgliedstaaten sollte es weiterhin freistehen, eine kürzere Frist festzulegen. Die Datenschutzgruppe hat schließlich Schutzvor-kehrungen im Hinblick auf die Voraussetzungen für den Zugang und zur Nutzung der Daten, die Notwendigkeit von Genehmigungen und Kontrollen sowie Maßnahmen zur Datensicherheit gefordert.

Wir haben auf Landesebene versucht, über die Senatskanzlei Einfluss auf die nationale Meinungsbildung zu nehmen. Der Berliner Senat hat sich unseren grundsätzlichen Bedenken aber nicht angeschlossen und hat im Bundesrat – mit der großen Mehrheit der anderen Bundesländer – die Richtlinie als notwendigen Schritt zur Verbesserung des Schutzes insbesondere vor terroristischen Gefährdungen begrüßt. Der Senat hat aber zugleich Regelungen über die Vernichtung von Daten nach Ablauf der Speicherfrist und größtmögliche technische Sicherheit zur Vermeidung von Missbrauch eingefordert.

Nach äußerst kontroversen Diskussionen um Dauer und Kosten der Speicherung, Art der zu speichernden Daten sowie Umfang der Straftaten hat die Mehrheit der EU-Parlamentarier im Dezember 2005 ihren zunächst heftigen Widerstand gegen die Pläne zur Vorratsspeicherung aufgegeben. Die Justiz- und Innenminister der EU haben einen Kompromissvorschlag ausgearbeitet, dem das EU-Parlament nunmehr die notwendige Zustimmung erteilt hat[117]. In dem jetzt vorliegenden Regelungswerk ist anders als im ursprünglichen Richtlinienentwurf eine Speicherfrist von mindestens sechs Monaten und höchstens zwei Jahren vorgesehen. Über den genauen Zeitraum sollen die Mitgliedstaaten ebenso entscheiden wie über die Frage, wer bei welchen „schweren“ Straftaten unter welchen Voraussetzungen auf die zu speichernden Daten zugreifen können soll. Damit ist jedenfalls das Ziel einer europäischen Harmonisierung verfehlt worden. Die *Bundesregierung* hatte sich im Vorfeld für eine Speicherfrist von sechs Monaten ausgesprochen. Zudem will die Bundesjustizministerin die Daten auch zur Verfolgung von Straftaten einsetzen, die mit Hilfe von Telefon oder Internet

116 Stellungnahme 113/2005 v. 21. Oktober 2005 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG v. 21. September 2005 - (KOM(2005)438 endg.

117 Richtlinie 2006/.../EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

begangen werden (z. B. telefonische Belästigung „Tele-Stalking“ oder Urheberrechtsverletzungen in Internet-Tausch-börsen). Das Europäische Parlament hatte eine strikte Begrenzung auf Ermittlungen bei den 32 gravierenden Straftaten gefordert, für die auch ein EU-Haftbefehl beantragt werden kann. Die Richtlinie sieht ferner keine Verpflichtung zur Speicherung erfolgloser Anrufversuche mehr vor. Zudem muss die Standortkennung im Mobilfunk nur zu Beginn eines Gesprächs aufgezeichnet werden, nicht aber während und am Ende der Verbindung. Daten, die Aufschluss über den Inhalt einer Kommunikation geben, sind explizit von der Speicherpflicht ausgenommen. Die Richtlinie, die bei Redaktionsschluss noch der Zustimmung des Rates bedürfte, ist nach ihrem In-Kraft-Treten binnen 18 Monate in nationales Recht umzusetzen.

Der jetzt erzielte Kompromiss ändert wegen der erheblichen Eingriffe in die Privatsphäre nichts an unseren grundsätzlichen Einwänden gegen die Vorratsspeicherung. Sie führt zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung. Eine freie und unbefangene Kommunikation wird nicht mehr möglich sein. Jede Person, die die angesprochenen Kommunikationswege nutzt, wird unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, ist zum Scheitern verurteilt. Derartige Datenbestände werden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnte. Bestes Beispiel ist die bereits erhobene Forderung der Unterhaltungsindustrie, die Daten auch für die Verfolgung von Urheberrechtsverletzungen, also rein kommerzielle Interessen, zu nutzen. Während die Vorschläge für eine verbindliche Vorratsdatenspeicherung anfangs mit der Gefahr terroristischer Anschläge begründet wurden, sollen die Daten nach den Vorschlägen der Bundesjustizministerin jetzt auch zur Bekämpfung von individuellem „Telefonterror“ genutzt werden können. Dabei enthält das Telekommunikationsrecht seit jeher Regelungen (z. B. zur Fangschaltung), die diesen Zweck erreichen, ohne die Kommunikationsdaten von Millionen unverdächtiger Telefonkunden routinemäßig speichern zu müssen.

Es stellt sich die Frage, ob ein so massiver Eingriff in das Telekommunikationsgeheimnis zur bloßen Vorsorge für in der Zukunft möglicherweise notwendige Strafverfolgungsmaßnahmen in Deutschland auf der Grundlage des Grundgesetzes und vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts überhaupt in deutsches Recht umgesetzt werden darf. In jedem Fall müssen die von der Richtlinie gewährten Spielräume im Sinne eines effektiven Grundrechtschutzes ausgeschöpft werden, damit die Eingriffe so gering wie möglich bleiben.

***Mobilfunk-Ortung* von Personen**

Die *Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“* des *„Düsseldorfer Kreises“* hat sich in ihren Sitzungen im Jahr 2005 zum wiederholten Mal mit Datenschutzproblemen bei standortbezogenen Diensten („Location Based Services“) im Mobilfunkbereich befasst[118]. Im Mittelpunkt der Diskussion standen diesmal Dienste zur Bestimmung des Aufenthaltsortes von Personen (sog. *Tracking-Dienste*). Mit deren Hilfe können zum Beispiel Eltern feststellen, wo sich ihre Kinder befinden, Arbeitgeber den aktuellen Standort von Außendienstmitarbeitern überprüfen oder Jugendliche ermitteln, wo sich ihre Freunde gerade aufhalten. Die Ortung erfolgt dabei über das Mobiltelefon, das die zu ortende Person mitführt. Ein im Netz angemeldetes (eingeschaltetes) Handy wird mit Hilfe der so genannten Zellen-Identifikationsnummer (Cell ID) insofern eindeutig lokalisiert, als sein Standort im Verhältnis zur nächsten Basisstation ermittelt werden muss, um jederzeit eine Verbindung herstellen zu können. Das eingeschaltete Handy wirkt wie ein Peilsender[119]. Der jeweilige Standort wird dem Nutzer des Tracking-Dienstes über eine Webseite im Internet angezeigt.

Solche Ortungsdienste dürfen in der Regel nur auf Basis einer informierten Einwilligung der zu ortenden Person betrieben werden. Dennoch bestehen erhebliche Missbrauchsmöglichkeiten, etwa wenn ein zur Ortung freigeschaltetes Mobiltelefon an Dritte weitergegeben wird, ohne dass diese von der Möglichkeit zur Ortung Kenntnis haben. Um dies auszuschließen oder zumindest zu reduzieren, hält die Arbeitsgruppe die Umsetzung der folgenden Maßnahmen für erforderlich:

- Senden einer SMS an das geortete Handy bei jeder Ortung,
- gelegentliche, zufallsgesteuerte Information darüber, dass der Ortungsdienst aktiv geschaltet ist,
- verbunden mit einer Beschreibung, wie der Dienst deaktiviert werden kann.

Die *Art. 29-Datenschutzgruppe* hat im November 2005 eine Stellungnahme zur Verwendung von Standortdaten verabschiedet, die sich ausführlich mit dem Problem der *Lokalisierung* von Minderjährigen und Arbeitnehmern befasst[120].

Lokalisierungsdienste im Mobilfunkbereich gewinnen immer mehr an Bedeutung. Wer sein Handy eingeschaltet hat, muss es allerdings nicht hinnehmen, dass er ohne sein Wissen permanent geortet und verfolgt

118 Zur Verarbeitung von Standortdaten nach dem Telekommunikationsgesetz vgl. JB 2004, 5.1
119 dazu schon JB 2000, 5.1
120 Opinion on the use of location data with a view to providing value-added services, WP 115 v. 25. November 2005

wird.

5.2 Teledienste

Entwurf für ein *Telemediengesetz*

Die Fortentwicklung der nationalen Medienordnung nimmt konkrete Formen an[121]. Seit Mai 2005 liegen Entwürfe für ein Telemediengesetz des Bundes und einen Rundfunkänderungsstaatsvertrag der Länder vor. Hierzu führten der Bund durch das Bundeswirtschaftsministerium und die Länder durch die Staatskanzlei Rheinland-Pfalz eine gemeinsame Anhörung der kommunalen Spitzenverbände, Fachkreise und Verbände durch. Im November 2005 wurden die weiterentwickelten Regelungswerke bei der Kommission in Brüssel notifiziert[122].

Die Gesetzgebungsinitiative hat zum Ziel, die bisher bestehenden unterschiedlichen Rechtsvorschriften für Informations- und Kommunikationsdienste bei weitgehender Beibehaltung des materiellen Rechts zusammenzufassen. Die geltenden Vorschriften des Teledienstegesetzes (TDG), des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrages sollen durch ein einheitliches Telemediengesetz (TMG) des Bundes weitgehend ersetzt werden. Soweit bei journalistisch-redaktionell gestalteten Diensten eine Gesetzgebungskompetenz der Länder besteht, sollen die dafür erforderlichen spezifischen Vorschriften im Rundfunkstaatsvertrag geregelt werden. Hinsichtlich der Datenschutzbestimmungen sind dabei umfassende dynamische Verweisungen auf das TMG vorgesehen.

Wir waren an den Beratungen einer Bund-Länder-Arbeitsgruppe „Datenschutz“ beteiligt, deren Ergebnisse als Grundlage für die Datenschutzregelungen im TMG-Entwurf dienen sollten. Ein zentraler Diskussionspunkt war dabei zunächst die Frage des Geltungsbereichs der Vorschriften. Nach den Vorstellungen des Bundeswirtschaftsministeriums ist zentrales Anliegen des neuen TMG, eine klarere Abgrenzung zwischen Informations- und Kommunikationsdiensten (Telemedien) auf der einen und Telekommunikationsdiensten auf der anderen Seite zu erreichen. Das Ministerium geht davon aus, dass bestimmte telekommunikationsgestützte Dienste, wie etwa der Internet-Zugang oder die E-Mail-Übertragung, zugleich auch den Telemediendiensten zuzurechnen sind, weil sie neben der reinen Übertragungsdienstleistung

121 dazu bereits JB 2003, 5.1; JB 2004, 5.2

122 vgl. Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG), Stand: 15. November 2005, und Neunter Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (9. Rundfunkänderungsstaatsvertrag), Stand:
15. November 2005

auch eine inhaltliche Dienstleistung umfassen. Bisher hätten daher sowohl die Datenschutzregelungen des Telekommunikationsgesetzes als auch die des TDDSG gegriffen. Um mehr Rechtsklarheit und eine bessere Handhabung der Vorschriften für die Anbieter zu erreichen, sollen neben den Vorgaben des Telekommunikationsgesetzes künftig nur noch bestimmte Datenschutzvorschriften des TMG auf diese Dienste angewendet werden (§ 10 Abs. 3 TMG-Entwurf). Dazu zählen das Koppelungsverbot bei einer datenschutzrechtlichen Einwilligung der Nutzer, die Möglichkeit der Datenverarbeitung zur Bekämpfung von missbräuchlichen Nutzungen und bestimmte Ordnungswidrigkeiten-Tatbestände.

Nicht gelöst ist mit diesem Vorschlag allerdings die praktisch äußerst relevante Frage der Aufsichtszuständigkeit. Während für die Datenschutzkontrolle von Telemedien die Aufsichtsbehörden der Länder zuständig sind, kommt dem Bund die Kontrollkompetenz für Anbieter von Telekommunikationsdienstleistungen zu. Es ist daher unzureichend, wenn die fraglichen Ange-bote nicht vollständig einer Regelungsebene zugeordnet werden, sondern nur einzelne Normen aus dem TMG in Bezug genommen werden. Auf diese Problematik haben die Aufsichtsbe-hörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) auf Initiative der Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“, deren Vorsitz wir innehaben, gegenüber dem Bundeswirtschaftsministerium ausdrücklich hingewiesen.

Ein weiterer strittiger Punkt in den Sitzungen der Bund-Länder-Arbeitsgruppe war die Frage der Auskunftserteilung an berechtigte Stellen durch die Anbieter von Telemediendiensten. § 13 Abs. 2 des Entwurfs ergänzt die bisher im TDDSG geregelte Befugnis zur Auskunftserteilung für Zwecke der Strafverfolgung. Damit wird der Kreis der Behörden, an die Bestandsdaten übermittelt werden dürfen, um die Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienst und den Militärischen Abschirmdienst erweitert. Die Vorschrift besagt allerdings nur, dass Diensteanbieter die aus der Aufgabenerfüllung im Bereich der Strafverfolgung sowie der Nachrichtendienste erwachsenden Auskunftsansprüche nicht aus datenschutzrechtlichen Erwägungen zurückweisen können. Die Anordnung der zuständigen Stellen erfolgt allein nach Maßgabe der hierfür geltenden Bestimmungen etwa in der Strafprozessordnung oder den Bundes- und Landesverfassungsschutzgesetzen. Darüber hinaus sieht der Entwurf aber auch eine Übermittlungsbefugnis zur Durchsetzung von Rechten am *geistigen Eigentum* vor. Auf diesem Wege soll offensichtlich der Boden für die Schaffung von gesetzlichen Auskunftsansprüchen privater Rechteinhaber gegenüber den Diensteanbietern bereitet werden. Ein solches Auskunftsrecht würde den Grundsätzen des Telemedien-Datenschutzes allerdings diametral zuwiderlaufen.

Erheblichen Bedenken begegnete aus Sicht des Datenschutzes auch die zunächst vorgesehene deutliche Erweiterung der Befugnisse zur Verarbeitung von Nutzungsdaten. Nach

einem früheren Entwurf sollte bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte dafür, dass Telemedien-Dienste in der Absicht in Anspruch genommen werden, die Dienste „in sonstiger Weise rechtswidrig zu Lasten des Diensteinhabers oder Dritter“ zu nutzen, die Verwendung personenbezogener Daten der Nutzer zu Zwecken der Rechtsverfolgung erlaubt sein. Diese Formulierung kommt einer Blankettnorm gleich, die mit dem Prinzip der Normen-klarheit und dem Grundsatz der Verhältnismäßigkeit nicht vereinbar ist. Eine solche Befugnis könnte dazu führen, dass sich Diensteanbieter veranlasst sehen, in einem Umfang Nutzungs-daten zu verarbeiten, der die eigentlich als Regelfall gedachte unverzügliche Löschung nach Ende des jeweiligen Nutzungsvorgangs zur Ausnahme macht. Eine Einschränkung hinsichtlich der Schwere der rechtswidrigen Inanspruchnahme zu Lasten Dritter wird nicht gemacht. Sie ist auch insoweit systemfremd, als sie nicht das Anbieter-Nutzer-Verhältnis betrifft, sondern das Verhältnis zwischen Nutzern und Dritten. Der jetzt vorliegende Entwurf verzichtet zu Recht auf die umstrittene Regelung.

Ebenfalls Abstand genommen wurde von den ursprünglich vorgesehenen Plänen zur Einführung von Mechanismen der Selbstregulierung und eines spezifischen Datenschutzaudits für Telemedien. In der Bund-Länder-Arbeitsgruppe wurde für eine branchenspezifische Selbstregulierung außerhalb von § 38 a BDSG kein Bedürfnis gesehen. Ebenso wenig hielt die Arbeitsgruppe ein eigenständiges Datenschutzaudit vor dem Hintergrund eines möglichen Datenschutzaudit-Gesetzes zu § 9 a BDSG für sachgerecht. Dieses lässt allerdings weiter auf sich warten.

Die geplante Neuregelung der Telemedien darf von den bewährten Grundsätzen des Multimedia-Rechts, insbesondere der Datensparsamkeit und der sofortigen Löschung der Nutzungsdaten nach dem Ende der Verbindung, nicht abrücken.

„Testberichte“ über Hochschullehrer im Internet

Ein Berliner Unternehmen betreibt eine Internet-Plattform für Produktinformation und Produktvergleich. Unter anderem besteht im Rahmen dieses Angebots für registrierte Nutzer die Möglichkeit, die Leistung von Hochschullehrern durch die Vergabe von Sternen und in Form von sog. Testberichten zu bewerten. Die Beurteilungen stehen jedermann zum Abruf über das Internet zur Verfügung.

Bei den zu beurteilenden Informationen handelt es sich um personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG. Dies gilt nicht nur für die Namen und Vornamen der Professoren sowie die Namen der jeweiligen Hochschule, sondern auch für die in den Testberichten enthaltenen

Werturteile. Sie dienen der Darstellung der persönlichen und sachlichen Verhältnisse einer Person und zählen damit zu den Angaben im Sinne der gesetzlichen Definition. Das Werturteil erschöpft sich, jedenfalls wenn es im praktischen Zusammenhang auf eine Person angewendet wird, gerade nicht darin, die Subjektivität des Urteilenden auszudrücken, sondern bezweckt überdies eine informative Aussage über den Betroffenen.

Das Unternehmen erhebt und speichert personenbezogen Daten auf einem mit dem Internet verbundenen Server. Jeder Abruf der auf den Internetseiten eingestellten Daten durch einen Nutzer des Angebots erfüllt den Tatbestand der Übermittlung nach § 3 Abs. 4 Nr. 3 b BDSG. Es ist das Bekanntgeben gespeicherter Daten an einen Dritten in der Weise, dass zum Abruf bereitgehaltene Daten durch einen Dritten abgerufen werden. Die Einstellung ins Internet erfolgt mit dem Ziel, dass diese Daten jedermann zugänglich gemacht werden. Auch ein unbestimmter Informationsadressat ist Dritter i. S. d. § 3 Abs. 8 Satz 2 BDSG.

Mangels Einwilligung der betroffenen Professoren beurteilt sich die Zulässigkeit dieser Datenerhebung, -speicherung und -übermittlung nach den für nicht-öffentliche Stellen (§ 2 Abs. 4 BDSG) geltenden Vorschriften der §§ 27 ff. BDSG. Das Erheben, Speichern und Übermitteln dient hier nicht lediglich als Mittel für die Erfüllung eigener Geschäftszwecke, wie es die Erlaubnistatbestände in § 28 BDSG voraussetzen, sondern ist Selbstzweck. Die Daten werden allein zum Zweck der späteren Übermittlung erhoben und gespeichert. Der Bewertung ist deshalb § 29 BDSG zugrunde zu legen. Adressaten dieser Norm sind – wie die nicht abschließende Aufzählung der vier „klassischen“ geschäftsmäßigen Datenverarbeitungszwecke „für Dritte“ in Absatz 1 Satz 1 deutlich machen soll – in erster Linie Unternehmen, die gewerbsmäßig mit personenbezogenen Daten handeln, z. B. Wirtschafts- und Handelsauskunfteien, Detekteien, Adresshandel, Informationsdienste. Das hier fragliche Angebot ist mit dem einer Auskunftei vergleichbar. Die Informationen sind automatisiert abrufbar und in einer Datenbank ähnlichen Struktur systematisch aufbereitet. Damit unterscheidet sich das Angebot deutlich von der Veröffentlichungen einzelner personenbezogener Daten etwa auf privaten *Homepages*. Die Tatsache, dass die Daten frei zugänglich über das Internet angeboten werden sollen, kann nicht zu einer anderen Beurteilung der Rechtslage führen. Angesichts der besonderen Gefährdungslagen für das Persönlichkeitsrecht der betroffenen Personen ist für eine Privilegierung gegenüber klassischen Auskunfteien kein Raum. Es sind daher die gleichen Bewertungsmaßstäbe anzulegen.

Die Erhebung und Speicherung der Professorenbewertungen in Form der Testberichte kann nicht auf § 29 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden. Es handelt sich weder um allgemein zugängliche Daten noch um veröffentlichungsfähige Daten im Sinne der Vorschrift. Vielmehr muss sich die Verwendung dieser Daten an den Vorgaben des § 29 Abs. 1 Satz 1 Nr. 1

BDSG messen lassen. Danach ist die Erhebung, Speicherung und Veränderung von Daten zum Zwecke der Übermittlung nur zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat. Dies beurteilt sich anhand einer am Verhältnismäßigkeitsgrundsatz ausgerichteten Abwägung der Interessen des Betroffenen und derjenigen der verantwortlichen Stelle bzw. potenzieller Empfänger (Dritter). Dabei muss bereits der zukünftige Verwendungs-zusammenhang der Daten mit berücksichtigt werden.

Gemessen an diesen Maßstäben ist schon die Erhebung und Speicherung der *Professoren-bewertungen* nicht gerechtfertigt. Zwar muss bei der gebotenen Interessenabwägung zugunsten einer Datenverarbeitung berücksichtigt werden, dass die Bewertung der Hochschullehrer nur ihre berufliche Funktion, d. h. die von ihnen angebotene „Dienstleistung“ betreffen soll. Zudem muss der persönlichkeitsrechtliche Schutz in dem Maße zugunsten der Meinungsfreiheit Dritter zurücktreten, wie der Betroffene sich selbst in die Sphäre der Öffentlichkeit begibt (hier: ein Amt im öffentlichen Dienst ausübt). Andererseits ist es den hier in Frage stehenden Bewertungen aber gerade immanent, dass sie zugleich untrennbar mit vielfältigen Werturteilen über die hinter der Dienstleistung stehende Privatperson einhergehen. Dies tritt besonders deutlich bei den Testberichten zu Tage, die nicht fachrelevante Eigenschaften, Verhaltensweisen, Gestiken und andere persönliche Charakteristika in den Vordergrund stellen und letztlich auch zu wesentlichen Punkten der Bewertungsgrundlage machen.

Zu Lasten der verantwortlichen Stelle fällt ferner ins Gewicht, dass die Testberichte keiner redaktionellen Bearbeitung oder sonstigen inhaltlichen Kontrolle unterliegen und wegen ihrer stark subjektiven Einfärbung in der Regel in ihren Aussagen auch nicht nachprüfbar sind. Wegen des großen Risikos von Missverständnissen und der Möglichkeit zu gezielter Negativbewertung mit gegebenenfalls diskriminierender Wirkung gefährdet die Veröffentlichung solcher Angaben die schutzwürdigen Belange der Betroffenen in gesteigertem Maße. Eine andere Bewertung ergibt sich auch nicht dadurch, dass sich der Anbieter in seinen Allgemeinen Geschäftsbedingungen vorbehält, unsachliche, unwahre oder beleidigende Inhalte von der Veröffentlichung auszuschließen. Mangels einer tauglichen Inhaltsprüfung durch den Betreiber schützt das Angebot selbst vor solchen Äußerungen nicht, die von der Meinungsfreiheit nicht mehr gedeckt sind (z. B. Schmähkritik, Formalbeleidigungen, unwahre Tatsachenbehauptungen). Es fehlt bereits an vorab festgelegten objektiven Kriterien für die Abfassung der Testberichte.

Das Angebot unterscheidet sich insofern deutlich von den in der Presse regelmäßig publizierten so genannten Hochschul- oder Professorenrankings, die in der Regel auf wissenschaftlichen Erhebungsmethoden basieren, welche gerade dazu dienen, subjektive Elemente von Bewer-

tungen zurückzustellen und vorgefundene Bewertungen zu verobjektivieren. Gleiches gilt für die in den Hochschulgesetzen geregelte Evaluation der Lehre. Sie fußen nicht auf der losen Zusammenfassung von Meinungen, sondern schließen es von vornherein aus, dass unsachliche Kriterien oder rein persönliche Motive, die in keinem Zusammenhang mit der eigentlich zu bewertenden Leistung stehen, maßgebenden Eingang in die Bewertungen finden.

Nicht zuletzt muss berücksichtigt werden, dass die hier zu bewertenden Informationen über das Internet weltweit für jedermann abrufbar und recherchierbar sind und damit eine enorme Breitenwirkung entfalten. Die personenbezogenen Daten können beliebig kopiert und vervielfältigt werden. Eine regelmäßige Löschungsfrist ist nicht vorgesehen. Die Aktualität der Daten kann nicht gewährleistet werden. Dies wirkt sich im Rahmen der Interessenabwägung ebenfalls zu Lasten einer Veröffentlichung aus.

Unabhängig von der Unzulässigkeit der Erhebung und Speicherung ist erst recht die Übermittlung der Professorenbewertungen beim konkreten Abruf durch die Nutzer des Angebots rechtswidrig. Da es sich nicht um listenmäßig oder sonst zusammengefasste Daten handelt, wäre die Übermittlung nach § 29 Abs. 2 Satz 1 Nr. 1 a und Nr. 2 BDSG nur zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse glaubhaft darlegt und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Diese Vorgaben erfüllt das Angebot nicht, da schon eine Überprüfung, ob derjenige, der sich mit Hilfe der Testberichte über einen Hochschullehrer informiert, tatsächlich ein berechtigtes Interesse an den veröffentlichten Daten hat, nicht erfolgt. Dies wäre allenfalls im Rahmen einer geschlossenen Benutzergruppe durch eine entsprechende Erklärung der jeweiligen Datenempfänger bei Abschluss eines Nutzungsvertrags realisierbar. Derzeit besteht die Möglichkeit zum Abruf aber auch für solche Personen, die keinerlei Verbindung zu der jeweiligen Hochschule aufweisen.

Im Übrigen stehen der Übermittlung aus den oben genannten Gründen auch schutzwürdige Interessen des Betroffenen entgegen, solange keine eindeutigen und beweisbaren Fakten, sondern Behauptungen und subjektive Einschätzungen übermittelt werden.

Das Vorhalten von Bewertungen der Leistung von Hochschullehrern in Form von Testberichten und ihre Bereitstellung zum Abruf über das Internet ist datenschutzrechtlich unzulässig. Wir haben das Unternehmen aufgefordert, das Angebot einzustellen. Vergleichbare Plattformen zur Bewertung von Personen im Internet müssen ebenfalls die gesetzliche Grundentscheidung in § 29 BDSG beachten.

Web Browser Caching

Die Internationale Arbeitgruppe Datenschutz in der Telekommunikation/International Working Group on Data Protection in Telecommunications (IWGDPT) hat sich auf ihrer 38. Sitzung am 6./7. September 2005 in Berlin mit dem Problem des Web Browser Caching („Zwischen-speicherung“) bei öffentlichen Internet-Zugängen, z. B. in *Internet-Cafés* befasst [123]. Alle gängigen Browser speichern vorübergehend Kopien der aufgerufenen Webseiten auf der Festplatte des Nutzerrechners. In Internet-Cafes besteht daher die Gefahr, dass nachfolgende Nutzer wie auch andere Personen (z. B. Betreiber des Internet-Cafés) auf die zwischengespeicherten Seiten zugreifen und auf diese Weise darin enthaltene personenbezogene Daten des Vornutzers ausspähen. Die Arbeitsgruppe fordert daher von den Betreibern öffentlicher Internet-Zugänge, technisch-organisatorisch sicherzustellen, dass alle personenbezogenen Daten, die während der Sitzung eines Nutzers gesammelt werden, nach dem Ende dieser Sitzung vollständig entfernt werden. Weiterhin sollte der Nutzer selbst die Möglichkeit haben, den Inhalt des „History“-Ordners zu löschen, bevor ein anderer Nutzer Zugang zum System erhält. Es sollte ferner ein Warnhinweis oder -signal (z. B. ein Popup-Fenster) vorgesehen werden, das den Nutzer auf die Löschungsmöglichkeit aufmerksam macht, bevor er sich abmeldet.

123 Arbeitspapier zu Web Browser Caching („Zwischenspeicherung“) von personenbezogenen Daten bei öffentlichen Internet-Zugängen (z. B. Internet-Cafés)

Lex specialis: *Auskunftsanspruch* nach § 4 Abs. 7 TDDSG

Die Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“ des „Düsseldorfer Kreises“ hatte sich auf die Anfrage eines Teledienste-Anbieters hin mit der Frage zu befassen, ob die im BDSG geregelten Ausnahmefälle, in denen die Pflicht zur Erteilung einer Auskunft über die zur Person des Betroffenen gespeicherten Daten entfällt, auch im Rahmen einer Auskunft nach dem TDDSG zur Anwendung kommen.

Rechtsgrundlage für den Auskunftsanspruch eines Nutzers gegenüber dem Anbieter eines Teledienstes ist § 4 Abs. 7 TDDSG. Das Verhältnis dieses Auskunftsanspruchs zu den allgemeinen Datenschutzbestimmungen im BDSG regelt § 1 Abs. 2 TDDSG. Danach finden die „jeweils geltenden Vorschriften für den Schutz personenbezogener Daten“ Anwendung, „soweit in diesem Gesetz nicht anderes bestimmt ist“. Der Auskunftsanspruch des TDDSG ist daher gegenüber dem allgemeinen Auskunftsanspruch nach § 34 BDSG eine speziellere Regelung, so dass kein Raum für eine Anwendung der über § 34 Abs. 4 BDSG geltenden Ausnahmen des § 33 Abs. 2 BDSG besteht. Diese Auslegung wird durch die Gesetzesbegründung bestätigt. Zur gleichlautenden Vorgängerregelung heißt es, der Auskunftsanspruch stelle sicher, dass der Nutzer „über das nach dem Bundesdatenschutzgesetz geltende Auskunftsrecht hinaus“ die über ihn und sein Pseudonym gespeicherten Daten elektronisch einsehen könne.

Nach dem Willen des Gesetzgebers können die für das BDSG geltenden Ausnahmen vom Auskunftsrecht im Anwendungsbereich des TDDSG also nur dann gelten, wenn dies in dem bereichsspezifischen Gesetz ausdrücklich vorgesehen ist. Eine entsprechende Änderung deutet sich an. In dem Entwurf für ein Telemediengesetz (siehe dazu bereits die vorstehenden Ausführungen) wird in der Auskunftsregelung die Vorschrift des § 34 BDSG explizit in Bezug genommen.

Im Übrigen wird die Befolgung des Auskunftsanspruchs den Anbieter eines Teledienstes auch nicht unverhältnismäßig beanspruchen, wenn er seinen gesetzlichen Löschungspflichten nachkommt. Das TDDSG verpflichtet die Anbieter insbesondere zur frühzeitigen Löschung von Nutzungsdaten wie IP-Adressen und Zugriffszeiten. Ist eine solche Löschung gesetzeskonform erfolgt, wird in vielen Fällen eine Auskunft über die konkret gespeicherten Daten nicht mehr möglich sein. Der Diensteanbieter kann allenfalls typisiert über seine Verarbeitung Auskunft erteilen. Hierüber hat er den Nutzer nach § 4 Abs. 1 TDDSG ohnehin vor der Nutzung in allgemeiner Form zu unterrichten.

Nach der derzeitigen Rechtslage kommen die Ausnahmeregelungen des BDSG bei einer

Auskunft nach dem TDDSG nicht zur Anwendung.

5.3 Medien

Neuordnung des Verfahrens zur Befreiung von der *Rundfunkgebührenpflicht*

Mit In-Kraft-Treten des 8. Rundfunkänderungsstaatsvertrags am 1. April 2005 wurde das Verfahren zur Befreiung von der Rundfunkgebührenpflicht neu geordnet. Seitdem haben wir zahlreiche Beschwerden betroffener Bürger über Verletzungen des Datenschutzes bei der Beantragung einer Gebührenbefreiung erhalten. Dies betraf vor allem die Übersendung des Bewilligungsbescheides über den Bezug von ALG II an die GEZ.

Sowohl die materiell-rechtlichen Voraussetzungen für die Befreiung als auch das zugrunde liegende Verwaltungsverfahren sind nunmehr abschließend in § 6 Rundfunkgebührenstaatsvertrag (RGebStV) geregelt. Über Anträge auf Befreiung von der Rundfunkgebührenpflicht entscheidet ausschließlich die örtlich zuständige öffentlich-rechtliche Landesrundfunkanstalt, d. h. in Berlin der Rundfunk Berlin-Brandenburg. Die Landesrundfunkanstalten haben die Gebühreneinzugszentrale (GEZ) mit der Bearbeitung der Anträge und der Verarbeitung der in diesem Zusammenhang anfallenden personenbezogenen Daten beauftragt. Die bisherigen Zuständigkeiten der Träger der Sozialhilfe (bezirkliche Sozialämter) bestehen nicht mehr[124].

Nach § 6 Abs. 1 RGebStV können sich Empfänger bestimmter Sozialleistungen (z. B. Sozialhife, ALG II, BAföG) und Menschen mit bestimmten Behinderungen auf Antrag von der Gebührenpflicht befreien lassen. Die Antragsteller sind gem. § 6 Abs. 2 RGebStV verpflichtet, das Vorliegen der Befreiungsvoraussetzungen durch Vorlage des jeweiligen Bescheides im Original oder in beglaubigter Kopie nachzuweisen. Die nach der Neuorganisation eingeführte weitgehend zentrale Bewilligung von *Rundfunkgebührenbefreiungen* führt dazu, dass die Antragsteller die Nachweise nur noch „vorlegen“ können, indem sie diese an die GEZ schicken. Da das Gesetz die Vorlage vollständiger Bescheide verlangt, erhält die GEZ auf diese Weise eine Vielzahl personenbezogener Daten, die sie für die Entscheidung über die Befreiung nicht benötigt. Dazu gehören bei Empfängern von *Arbeitslosengeld II* beispielsweise umfangreiche Informationen über die Einkommens- und Vermögensverhältnisse sowie die Wohnsituation der Antragsteller und nicht selten ihrer Familienangehörigen. Erforderlich sind für die GEZ hingegen nur die Informationen über die Art der bewilligten Sozialleistung, der

124 zu dem bisherigen Verfahren JB 2004, 5.3

Bewilligungszeitraum sowie bei einigen Befreiungstatbeständen bestimmte Zusatzinformationen.

Die Pflicht, Bescheide beglaubigen zu lassen und der GEZ vollständig ohne jede Erforderlichkeit zur Verfügung stellen zu müssen, stößt bei den Betroffenen daher zu Recht auf Unverständnis. Der Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder hat ein datenschutzgerechtes und vor allem datensparsames Verfahren zum Nachweis der Befreiungsvoraussetzungen vorgeschlagen. Danach soll auf dem Antragsformular für die Gebührenbefreiung die Möglichkeit vorgesehen werden, die für die Befreiung erforderlichen Daten aus den Nachweisen einzutragen und durch die jeweils bewilligende Behörde bestätigen zu lassen. Die hierfür notwendige Änderung des § 6 Abs. 2 RGebStV könnte im Rahmen des jetzt anstehenden 9. Rundfunkänderungsstaatsvertrags erfolgen. Der Arbeitskreis Medien hat dies gegenüber den Rundfunkreferenten der Länder angeregt.

Die derzeitige Ausgestaltung des Verfahrens zur Befreiung von der Rundfunkgebührenpflicht verstößt gegen datenschutzrechtliche Grundsätze. Bis zu einer Änderung der Rechtslage empfehlen wir den betroffenen Bürgern, die jeweilige Sozialbehörde um eine Bescheinigung zu bitten, die sich auf die notwendigen Daten beschränkt, oder die nicht erforderlichen Daten auf der Kopie des Bewilligungsbescheids vor der Versendung an die GEZ selbst zu schwärzen.

6. Informationsfreiheit

6.1. Informationsfreiheit auf Bundesebene

Kurz vor dem Ende der letzten Legislaturperiode wurde endlich der Weg für ein *Informationsfreiheitsgesetz des Bundes*[125] freigemacht. Entgegen den Ausschussempfehlungen zur Anrufung des Vermittlungsausschusses ließ der Bundesrat das von Rot-Grün vorbereitete Reformvorhaben passieren, nachdem die Vertreter der von der FDP mitregierten Länder im Bundesrat sich der Abstimmung enthielten. Das Gesetz ist am 1. Januar 2006 in Kraft getreten. Der Bundesbeauftragte für den Datenschutz ist nun zugleich Bundesbeauftragter für die Informationsfreiheit. Mit dem Erlass des Gesetzes ist die Hoffnung verbunden, dass weitere Gesetzentwürfe auf Landesebene (z. B. in Bremen, Hamburg, Mecklenburg-Vorpommern und im Saarland) „Anschub“ erhalten. Das unterschiedliche *Transparenzniveau* in der deutschen Verwaltung sollte alsbald zugunsten der Bürger vereinheitlicht werden.

125 v. 5. September 2005, BGBl. I, 2722

Mit dem *Gesetz über die Offenlegung der Vorstandsvergütungen (Vorstandsvergütungs-Offenlegungsgesetz - VorstOG)*[126] wurde die gesetzliche Pflicht zur Offenlegung individueller Vorstandsvergütungen durch Änderung des Handelsgesetzbuchs festgelegt. Das Gesetz war die Reaktion auf die Weigerung eines Teils der im Deutschen Aktienindex (DAX) notierten Unternehmen, im Wege der freiwilligen Selbstverpflichtung im Rahmen des Corporate Governance Kodexes die Bezüge transparent zu machen[127]. Damit soll bei börsennotierten Aktiengesellschaften die Feststellung erleichtert werden, ob die Bezüge in einem angemessenen Verhältnis zu den Aufgaben des Vorstandmitglieds und zur wirtschaftlichen Situation der Gesellschaft stehen. Zugleich ist die Information für den Anleger wichtig und verbessert den Anlegerschutz. Das Gesetz ist ein Anwendungsfall der Informationsfreiheit bei privaten Stellen, die von den allgemeinen Informationsfreiheitsgesetzen grundsätzlich nicht umfasst ist.

Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID) hat die Gesetzgeber des Bundes und der Länder aufgefordert, eine entsprechende Offenlegungspflicht auch für öffentlich kontrollierte Unternehmen festzulegen[128]. Weitergehend hat die AGID die Gesetzgeber in den Ländern aufgefordert, „nebenamtliche“ Aktivitäten und Vergütungen öffentlicher Entscheidungsträger gesetzlich festzulegen, die den Vorsitz in einer bestimmten Organisation führen oder in einem Aufsichtsrat eines Unternehmens sitzen[129]. In Zeiten, in denen die öffentlichen Stellen aufgerufen sind, verstärkt *Korruption* im eigenen Haus zu bekämpfen, ist es erforderlich, dass Mitglieder kommunaler Vertretungen und der Landesregierungen verpflichtet werden, über ihre Tätigkeit in einer Organisation oder einem privaten Unternehmen und dafür erlangte zusätzliche Vergütungen Auskunft zu geben.

In Umsetzung der Europäischen Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors[130] hat das Bundesministerium für Wirtschaft und Arbeit den *Entwurf eines Gesetzes über die Weiterverwendung von Informationen öffentlicher Stellen (Informations-weiterverwendungsgesetz – IWG-E)* erarbeitet. Vorrangiges Ziel ist die Erschließung des wirtschaftlichen Potenzials, das in den Informationen öffentlicher Stellen liegt. Der Entwurf begründet kein eigenständiges Zugangsrecht zu Informationen, sondern knüpft an solche Informationen an, die öffentliche Einrichtungen bereits zur Verfügung stellen. Er baut damit auf bestehenden Zugangsregelungen von Bund und Ländern auf.

---

126 v. 3. August 2005, BGBl. I, 2267

127 JB 2004, 4.9.3

128 Entschließung „Transparenz in öffentlichen Unternehmen gefordert“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 114

129 Entschließung „Offenlegung von Aktivitäten und Bezügen der Mitglieder öffentlicher Organe und Gremien“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 115

130 2003/98/EG v. 17. November 2003; vgl. JB 2004, 4.9.2

Obgleich das IFG und der IWG-E unterschiedliche Ziele verfolgen, ist eine Abgrenzung schwierig, weil letzterer (richtlinienkonform) nicht zwischen einer wirtschaftlichen Weiterverwendung der erlangten Informationen und einer Nutzung zu privaten, politischen oder sonstigen Zwecken unterscheidet. Als „*Weiterverwendung*“ wird in § 4 Nr. 3 IWG-E jede wirtschaftliche und anderweitige Nutzung von Informationen definiert, die über die Erfüllung einer öffentlichen Aufgabe hinausgeht. Die nicht-kommerzielle Nutzung von Informationen durch Private entspricht aber zugleich Sinn und Zweck des IFG, das – anders als der IWG-E - von einem begründungsfreien Recht auf Informationszugang ausgeht. Wer privat eine Datenbank zu bestimmten Themen des öffentlichen Interesses anlegt und sie mit Informationen öffentlicher Stellen anreichern will, kann diesbezüglich sowohl nach dem IFG als auch dem IWG-E vorgehen.

Eine Abgrenzung ist aber erforderlich, um die Funktionen des IFG durch die primär wirtschaftlich ausgerichteten Regelungen des IWG-E nicht zu beeinträchtigen. Bei einer Schnittmenge des Informationszugangs und der Informationsweiterverwendung bestünde die Gefahr, dass eine öffentliche Stelle bereits den (nach IFG begründungsfreien) Informationszugang unter Verweis auf die Regelungen des IWG ablehnt oder geneigt ist, eine Weiterverwendung nach IWG zu bejahen, um höhere Gebühren erheben zu können. Denn im Unterschied zum IFG darf für Informationen nach dem IWG-E ein Entgelt erhoben werden, das sich an einer Kostendeckung zuzüglich einer angemessenen Gewinnspanne orientiert. Eine Ablehnung des Informationsgesuches wäre nach IWG-E möglich, wenn noch keine Weiterverwendung der begehrten Informationen stattfindet, die „Erstgestattung“ der Weiterverwendung also Gegenstand eines Antrages ist. Den Begriff der „Weiterverwendung“ richtlinienkonform auf Informationsprodukte mit Mehrwert zu beschränken, bietet für die Abgrenzung des IWG-E vom IFG nur eine scheinbare Lösung, weil ein unklarer Rechtsbegriff durch einen anderen ersetzt würde.

Das Dilemma der Abgrenzung kann aber aufgelöst werden, indem eine Schnittmenge der Anwendungsbereiche von IWG-E und IFG akzeptiert und seine Anwendung über die Öffnungsklausel des § 3 Abs. 3 IWG-E ermöglicht wird. Danach bleiben weitergehende Ansprüche auf Weiterverwendung von Informationen öffentlicher Stellen unberührt. Da das IFG einen begründungsfreien Anspruch vorsieht und die öffentliche Stelle einen Gewinn durch Preisgabe der Informationen nicht erzielen darf, entspricht der Anspruch nach IFG diesen Vorgaben zumindest bei nicht-kommerziellen Informationsgesuchen. Dagegen widerspricht das in § 13 Abs. 7 des Berliner Informationsfreiheitsgesetzes enthaltene Verbot der wirtschaftlichen Nutzung von Informationen den Vorgaben der Richtlinie 2003/98/EG und sollte gestrichen werden. Eine vergleichbare Vorschrift enthalten weder die Informationsfreiheitsgesetze des Bundes noch der anderen drei Länder. Praktisch könnte das bedeuten, dass nicht-kommerzielle

Informationsgesuche weiterhin ausschließlich nach dem IFG (als lex specialis) zu behandeln wären, kommerzielle Begehren dagegen nach dem neuen IWG. Wir haben diese Auffassung der Senatsverwaltung für Wirtschaft, Arbeit und Frauen mitgeteilt, die uns um Stellungnahme zum IWG-E gebeten hatte.

6.2 Informationsfreiheit im Land Berlin

In Berlin wurde die Offenlegungspflicht für Bezüge der Vorstandsmitglieder landeseigener Anstalten im *Vergütungs- und Transparenzgesetz* festgelegt[131]. In den neuen Paragraphen §§ 16 a Berliner Betriebegesetz und 65 a Landeshaushaltsordnung wurden die Einzelheiten zur Offenlegung der *Vorstandsvergütungen* sowie der Vergütung der Mitglieder des Geschäftsführungsorgans festgelegt.

Ein weiteres Signal für mehr Transparenz bei (Neben-)Tätigkeiten und Vergütungen sind die „Verhaltensregeln für Mitglieder des Abgeordnetenhauses“, die in § 5 a *Landesabgeordneten-gesetz* aufgenommen worden sind[132]. Danach müssen Abgeordnete künftig im Handbuch und Internetauftritt des Abgeordnetenhauses u. a. offen legen, welche Tätigkeiten sie neben ihren parlamentarischen Aufgaben ausüben. Die Einkünfte durch diese Tätigkeiten müssen sie unter bestimmten Voraussetzungen dem Präsidenten des Abgeordnetenhauses anzeigen.

Die *Umsetzung der Umweltinformationsrichtlinie*[133] wurde durch Änderung des Berliner Informationsfreiheitsgesetzes (IFG) vorgenommen[134]. Der neue § 18 a IFG regelt nunmehr den Zugang zu Umweltinformationen im Land Berlin und verweist weitestgehend auf das Bundesumweltinformationsgesetz. Die Zusammenführung der landesrechtlichen Regelung mit dem IFG entspricht unserer Forderung nach übersichtlichen Informationsrechten zugunsten einer besseren Transparenz für den Bürger[135]. Das neue IFG ist am 31. Dezember 2005 in Kraft getreten. Unsere Schiedsstellenfunktion erstreckt sich fortan auch auf den Zugang zu Umweltinformationen.

Zur besseren Handhabung der *Gebührenregelung für Amtshandlungen nach IFG* haben wir in

131 Gesetz zur Herstellung von Transparenz bei den Vorstandsvergütungen der Berliner Anstalten und den Geschäftsführungsvergütungen bei Beteiligungen Berlins an privatrechtlichen Unternehmen v. 23. September 2005, GVBl., 475
132 Sechzehntes Gesetz zur Änderung des Landesabgeordnetengesetzes v. 3. November 2005, GVBl., 690
133 Richtlinie 2003/4/EG über den Zugang der Öffentlichkeit zu Umweltinformationen
134 Erstes Gesetz zur Änderung des Berliner Informationsfreiheitsgesetzes v. 19. Dezember 2005, GVBl., 791
135 JB 2004, 4.9.3

Zusammenarbeit mit der Senatsverwaltung für Inneres eine *Gebührenstaffel* entworfen[136]. Sie unterscheidet zwischen der Gebühr bei mündlichen Auskünften, bei der Erteilung einer einfachen schriftlichen Auskunft, bei der Erteilung einer umfangreichen schriftlichen Auskunft und bei der Erteilung einer schriftlichen Auskunft verbunden mit außergewöhnlichem Verwaltungsaufwand. Während mündliche Auskünfte gebührenfrei sind, beträgt die Gebühr in den übrigen Fällen 0–100 Euro, 100–255 Euro und 250–510 Euro. Leider hat die Senatsverwaltung für Finanzen es bisher nicht für erforderlich gehalten, die geltende Tarifstelle 1004 in der Verwaltungsgebührenordnung entsprechend zu ändern. Dem wurde dadurch Vorschub geleistet, dass die Senatsverwaltung für Inneres im Zuge der Änderung des Berliner Informationsfreiheitsgesetzes anlässlich der Umsetzung der Umweltinformationsrichtlinie – trotz des mit uns erarbeiteten Entwurfs der Gebührenstaffel – von einer unveränderten Tarifstelle 1004 in der Verwaltungsgebührenordnung ausgegangen ist. Dies war insofern widersprüchlich, als die federführend von der Senatsverwaltung für Inneres erarbeitete Gesetzesvorlage zur Änderung des IFG zwar den weitgehenden Verweis auf das Bundesumweltinformationsgesetz vorsah, jedoch nicht auf die dort geltende bürgerfreundliche Gebührenstaffel. Damit entstand der Eindruck, dass der grundsätzliche Widerstand der Senatsverwaltung für Inneres gegen eine Gebührenstaffel nach wie vor nicht aufgegeben war. Die Beratungen im Unterausschuss „Datenschutz und Informationsfreiheit“ haben ergeben, dass entweder die Gebührenregelung des Bundesumweltinformationsgesetzes in Landesrecht übernommen oder die mit der Senatsverwaltung für Inneres erarbeitete Gebührenstaffel eingeführt wird[137]. Die Fraktionen vereinbarten, einen gesonderten Antrag zur Änderung der Verwaltungsgebührenordnung im letztgenannten Sinne einzubringen[138].

Informationszugang beim RBB

Ein Petent begehrte beim Rundfunk Berlin-Brandenburg (RBB) Auskunft über die Bedeutung der Abkürzungen im Feld „Abmeldegründe“ in den von der GEZ verwendeten Datenverarbeitungsmasken. Dies lehnte der RBB unter Berufung auf § 7 Satz 1 IFG ab. Bei der Aufschlüsselung der Abmeldegründe handele es sich um ein „Betriebsgeheimnis“. Die Kenntnis der akzeptierten Abmeldegründe könne zu einer gezielten und massenhaften Aushebelung der Gebührenpflicht führen. Nachdem der RBB aufgrund unserer Intervention die Bedeutung der Abmeldegründe kundgetan hatte, veröffentlichte der Petent unseren Schriftwechsel mit dem RBB auf seiner Homepage, in der auch für seine beiden Broschüren „Zur Problematik des Gebühreneinzugs durch die GEZ“ geworben wurde.

136 JB 2004, 4.9.4; JB 2001, 4.9
137 Beschlussprotokoll der Sitzung v. 16. August 2005
138 Beschlussprotokoll der Sitzung v. 25. Oktober 2005

Wir haben dem RBB mitgeteilt, dass der Anwendungsbereich des § 7 Satz 1 IFG nicht eröffnet ist. Öffentliche Stellen sind Adressaten des IFG und können sich grundsätzlich nicht auf den Schutz von Betriebs- und Geschäftsgeheimnissen berufen und den Informationszugang nicht aus diesem Grunde verweigern. Allein bei fiskalischem Handeln der öffentlichen Stelle kann im Einzelfall die Berufung auf eigene Betriebs- und Geschäftsgeheimnisse erfolgen. Der RBB (und in seinem Auftrag die GEZ) handelt hier aber nicht fiskalisch, sondern bei der Überprüfung und Durchsetzung der Gebührenpflicht hoheitlich. Die Maßstäbe, die dem hoheitlichen Handeln der öffentlichen Stelle generell zugrunde gelegt werden und der Entscheidungsfindung dienen, dürfen in einem Rechtsstaat nicht geheim gehalten werden. Welche Maßstäbe dies sind, ergibt sich auch aus der Bedeutung der Kürzel der Abmeldegründe. Sie unterliegen damit der Informationsfreiheit. Rechtsgrundlage für die Überlassung unseres Schriftwechsels mit dem RBB an den Petenten ist § 6 Abs. 1 i. V. m. Abs. 2 Satz 1 Nr. 2 IFG. Ein Verbot zur Veröffentlichung der erhaltenen Informationen nach § 13 Abs. 7 IFG liegt nicht vor. Gewerbliche Zwecke im Sinne dieser Vorschrift werden nur dann verfolgt, wenn die Nutzung der erhaltenen Informationen in (primärer) Gewinnerzielungsabsicht erfolgt, etwa wenn ein Bürger Informationen von öffentlichen Stellen erhält, um systematisch Datenbanken anzulegen und sie Dritten zur kostenpflichtigen Nutzung anzubieten. Hier hat der Petent nicht in Gewinnerzielungsabsicht gehandelt, sondern mit der Intention, über die Haltung des RBB und der GEZ in Bezug auf den Umgang mit dem Informationsfreiheitsgesetz zu informieren. Der RBB teilt diese Rechtsauffassung nicht und hat angekündigt, künftig bereits wegen § 10 Abs. 3 Ziffer 2 IFG den Informationszugang zu verweigern, „da die Zustimmung der übrigen an der GEZ beteiligten Rundfunkanstalten in aller Regel nicht vorliegen wird."

Auch dieses Argument geht allerdings fehl. Der RBB ist als Auftraggeber der GEZ allein dafür verantwortlich, aus welchen Gründen er jemanden von der Pflicht zur Zahlung der Rundfunkgebühr befreit. Auf Angaben oder Mitteilungen anderer Rundfunkanstalten, die nicht dem IFG unterliegen, kommt es deshalb nicht an.

Adressaten des IFG können sich grundsätzlich nicht auf den Schutz von Betriebs- und Geschäftsgeheimnissen berufen. Allgemeine Bewertungsgrundlagen für hoheitliches Handeln dürfen in einem Rechtsstaat nicht geheim gehalten werden.

Eine Petentin begehrte beim RBB den Informationszugang zu den Hinweisen zur

Befreiung von der Rundfunkgebührenpflicht, die als „Kriterienkatalog 2004“ in einem Handbuch an die Behörden ausgegeben wurden. Der RBB übersandte das Inhaltsverzeichnis der Hinweise an die Petentin, nicht jedoch die Hinweise selbst und berief sich dabei auf § 10 Abs. 4 IFG. Aufgrund ihres internen Charakters seien die Hinweise der Öffentlichkeit nicht zugänglich. Sie dienten allein der Entscheidungsfindung durch den RBB. Eine beschränkte Akteneinsicht nach § 12 IFG komme nicht in Betracht, da die Trennung der nicht zur Veröffentlichung geeigneten Aktenteile von den sonstigen für den RBB mit einem unverhältnismäßigen Aufwand verbunden wäre. Das Inhaltsverzeichnis sei aus Kulanz an die Petentin geschickt worden. Die Angelegenheit habe sich inzwischen ohnehin erledigt, da die Hinweise seit dem 1. April 2005 wegen des 8. Rundfunkänderungsstaatsvertrages keine Gültigkeit mehr hätten.

Die Voraussetzungen von § 10 IFG, der den Informationszugang zugunsten des Schutzes des behördlichen Entscheidungsprozesses einschränkt bzw. ausschließt, liegen hier nicht vor. Zum einen ist der Entscheidungsprozess nur im Einzelfall geschützt. Die Petentin begehrt jedoch nicht Einsicht in einen konkreten Vorgang, sondern allgemein Auskunft über die in einer Vielzahl von Fällen angewandten Hinweise. Zum anderen war der Prozess der Willensbildung nach der eigenen Argumentation des RBB abgeschlossen. Mit Beendigung des Prozesses entfällt die mit § 10 IFG in Bezug auf den behördlichen Entscheidungsprozess beabsichtigte Schutzbedürftigkeit. Interne Behördenvorgänge auch nach deren Erledigung dem öffentlichen Zugriff zu entziehen, würde bedeuten, dass für die Anwendung des IFG kein Raum bliebe. Denn faktisch können alle Behördenvorgänge als intern bezeichnet werden. Die Ablehnung der beschränkten Akteneinsicht nach § 12 IFG wegen unverhältnismäßigen Aufwandes ging fehl, denn die Vorschrift kennt eine solche Einschränkung nicht. Auch konnte angesichts von (laut Inhaltsverzeichnis) 40 Seiten nicht von einem unverhältnismäßigen Aufwand ausgegangen werden. Die Petentin hat angekündigt, gegen die Entscheidung den Rechtsweg zu beschreiten.

Nach § 10 IFG ist der Entscheidungsprozess nur im Einzelfall geschützt. Die Schutzbedürftigkeit entfällt, wenn der Entscheidungsprozess beendet ist. Für die Gewährung des beschränkten Informationszugangs nach § 12 ist der Aufwand der Behörde unerheblich.

Geschäftsverteilungspläne und *Statistiken* unter Verschluss?

Ein Petent hat beim Generalstaatsanwalt bei dem Kammergericht die Einsicht in die Geschäftsverteilungspläne der Generalstaatsanwaltschaft sowie der Staatsanwaltschaft Berlin beantragt und Auskunft begehrt, ob dort statistische Erhebungen vorhanden seien. Der Generalstaatsanwalt hat den Einsichtsantrag zunächst mit der Begründung zurückgewiesen, ihm sei ein nachvollziehbares Interesse nicht zu entnehmen. Später wurde eine nach § 12 IFG beschränkte Akteneinsicht zugestanden. Die vollständige Bekanntgabe der Geschäftsverteilung mit Nennung der Behördenangehörigen wurde unter Hinweis auf deren schutzwürdigen Belange nach § 6 Abs. 1 IFG verweigert. Die Auskunft, ob Statistiken vorhanden seien, wurde nicht erteilt mit der Begründung, das IFG enthalte hierfür keine Rechtsgrundlage. Darüber hinaus obliege es dem Antragsteller, den Gegenstand seines Auskunftsersuchens näher zu bezeichnen. In Anbetracht des „nicht unbeträchtlichen Umfangs der Geschäftsverteilungspläne“ wurde eine Gebühr von mindestens 150 € in Aussicht gestellt.

Nach § 3 Abs. 1 Satz 1 IFG hat jeder Mensch nach seiner Wahl ein Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten. Dieses Informationsrecht ist „voraussetzungslos“, d. h. der Antragsteller braucht sein Interesse an den Informationen grundsätzlich nicht zu begründen.

Die Auffassung, nach der die Nennung der Behördenangehörigen unter Hinweis auf ihre schutzwürdigen Belange nach § 6 Abs. 1 IFG unterbleiben muss, ist unzutreffend. Sie verkennt, dass der Gesetzgeber in § 6 Abs. 2 IFG bereits die Abwägung getroffen hat, in welchen Fällen schutzwürdige Belange der Betroffenen der Offenbarung ihrer personenbezogenen Daten nicht entgegenstehen. Nach der Wertung des Gesetzgebers sind personenbezogene Daten von Amtsträgern in der Regel gerade nicht schutzbedürftig (§ 6 Abs. 2 Satz 1 Nr. 2 IFG). Ausnahmen von dieser Regel aufgrund einer Bedrohung einzelner Staatsanwälte hat der Generalstaatsanwalt nicht dargelegt.

Statistiken sind nach der „Anordnung über die Erhebung von statistischen Daten bei den Staats- und Amtsanwaltschaften (StA-Statistik)“ zu führen und gehören zu den Aufzeichnungen, die nach § 3 Abs. 1 und 2 IFG dem Informationszugang unterliegen. Für den Fall, dass dem Antragsteller Angaben zur hinreichenden Bestimmung einer Akte fehlen, trifft die öffentliche Stelle eine Beratungs- und Unterstützungspflicht (§ 13 Abs. 1 Satz 2 IFG). Zwar sind alle öffentlichen Stellen in Berlin verpflichtet, ihre Aktenpläne zu veröffentlichen (§ 17 Abs. 4 Satz 2 IFG); dies hat sich aber offenbar noch nicht allgemein herumgesprochen. Auch deshalb kann von keinem Bürger erwartet werden, dass er die Aktenordnung einer Behörde kennt, von der er

Informationen verlangt. Diese hat ggf. durch Rückfrage bei ihm zu ermitteln, um welche konkreten Angaben es ihm geht.

Die in Aussicht gestellte *Gebühr* erschien nicht nachvollziehbar und überhöht. Die angegebene Begründung konnte ihrer Art nach allenfalls für die Anzahl der in Rechnung zu stellenden Fotokopien herangezogen werden. Im Übrigen dürfen nach der Rechtsprechung des EuGH zum vergleichbaren *Umweltinformationsrecht*[139] Gebühren, die dem Bürger für den Informationszugang in Rechnung gestellt werden, nicht prohibitiv wirken, d. h. sie dürfen nicht so berechnet sein, dass der Bürger von vornherein davon abgehalten wird, von seinem Informationszugangsrecht Gebrauch zu machen. Wir haben den Generalstaatsanwalt bei dem Kammergericht auf unsere Rechtsauffassung hingewiesen. Eine abschließende Stellungnahme steht noch aus.

Personenbezogene Daten von Amtsträgern unterliegen dem Informationszugang ebenso wie vorhandene Statistiken. Die Gebühr darf auf den Bürger nicht prohibitiv wirken.

Akteneinsicht bei Botschaftsgrundstücken?

> *Ein Bezirksamt wollte wissen, ob der Akteneinsicht für Grundstücke mit ausländischen Vertretungen die „Gemeinwohlklausel“ des § 11 IFG entgegensteht. Angesichts der Tatsache, dass die Bauakten Konstruktionszeichnungen mit statischen Angaben und Darstellungen der Grundrisse umfassen, seien Schutzbedürfnisse des jeweiligen Staates tangiert. Der Informationszugang könne theoretisch auch der Vorbereitung von Übergriffen auf die jeweiligen Grundstücke dienen.*

Nach § 11 (letzter Fall) IFG darf die Akteneinsicht nur versagt werden, wenn das Bekannt-werden des Akteninhalts zu einer schwer wiegenden Gefährdung des Gemeinwohls führen würde. Bei der *„Gemeinwohlklausel“* handelt es sich um einen eng auszulegenden Ausnahme-tatbestand. Deshalb ist er nur erfüllt, wenn im Einzelfall mit hinreichender Wahrscheinlichkeit Leben, Gesundheit oder Freiheit gefährdet würden. Eine nur abstrakte Gefährdung wie im vorliegenden Fall reicht nicht aus. Primär wäre aber der Versagungstatbestand des § 10 Abs. 3 Ziffer 2 IFG zu berücksichtigen. Danach besteht das Recht auf Akteneinsicht oder Aktenaus-kunft nicht, soweit durch das Bekanntwerden des Akteninhalts Angaben und Mitteilungen öffentlicher Stellen, die nicht dem Anwendungsbereich dieses

139 Entscheidung v. 9. September 1999, NVwZ 1999, 1209, 1211

Gesetzes unterfallen, ohne deren Zustimmung offenbart werden. Davon ausgehend, dass die Konstruktionszeichnungen und Darstellung der Grundrisse im Auftrag der ausländischen Stelle angefertigt werden, haben wir die Auffassung vertreten, dass es sich um deren Angaben handelt. Deshalb dürfen ohne deren Zustimmung die Angaben nicht offenbart werden. Im Umkehrschluss bedeutet dies, dass das Bezirksamt versuchen muss, die entsprechende Zustimmung bei der ausländischen Vertretung einzuholen.

Eine nur abstrakte Gefährdung des Gemeinwohls erfüllt nicht den Tatbestand des § 11 IFG.

7. Aus der Dienststelle

7.1 Entwicklung

Dieser Bericht dokumentiert, dass die Aufgaben und Herausforderungen der Dienststelle im vergangenen Jahr deutlich zugenommen haben. Die Europäische Kommission hat schon im Mai 2003 hervorgehoben, dass eine hinreichende Personalausstattung der Kontrollstellen für den Datenschutz wesentliche Voraussetzung für deren Unabhängigkeit ist[140]. Die Kommission hat dies erneut unterstrichen im Vorfeld der jetzt in Deutschland erfolgten Einführung von Reisepässen mit biometrischen Merkmalen: Ohne personell und technisch hinreichend ausgestattete und damit unabhängige Datenschutzbehörden ist die permanente Ausweitung der Verarbeitung von – teilweise sensitiven – Bürgerdaten nicht zu verantworten.

Vor diesem Hintergrund ist es zu begrüßen, dass das Abgeordnetenhaus von Berlin dem Vorschlag meines Amtsvorgängers gefolgt ist und trotz der äußerst schwierigen Haushaltslage den Stellenplan der Dienststelle aufgestockt hat. Damit sind die Voraussetzungen dafür geschaffen, dass die Dienstelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit auch weiterhin als Kompetenzzentrum für Bürger, Verwaltung und Unternehmen wirken kann.

Im Berichtszeitraum schied ein langjähriger Mitarbeiter in unserem Bereich Informatik, Herr Dipl.-Physiker Joachim Laß, aus und trat in den Ruhestand. Aus der Bürgerbewegung der früheren DDR kommend war er 1990 unmittelbar nach der Wende zu uns gestoßen und hatte seitdem wesentlichen Anteil daran, dass die Dienststelle (seinerzeit) des Berliner Datenschutzbeauftragten als Bürgerbehörde wahrgenommen wurde. Seine Hauptaufgabengebiete waren Überwachungssysteme (insbesondere Videoüberwachung), Probleme der Biometrie, Payment-Systeme und die Organisation von Rechenzentren.

7.2 BürgerOffice

Das BürgerOffice hat sich als zentrale Anlaufstelle für Bürgerinnen und Bürger in unserer Behörde bewährt. Es stellt sicher, dass eine zentrale gesetzliche Aufgabe des Datenschutzbeauftragten, Beschwerden nachzugehen und wenn möglich abzuhelfen, effektiv und unabhängig von den sonstigen Aufgabenbereichen wie Beratung und Kontrolle von Verwaltungen und Unternehmen erledigt wird.

---

140 Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG/95/46) v. 15. Mai 2003, http://www.europa.eu.int/eur-lex/de/com/rpt/2003/com2003_0265de01.pdf

Die Zahl der Bürgereingaben stieg auch im vergangenen Jahr weiter an, wobei ein besonders starker Anstieg der Beschwerden über private Datenverarbeiter zu beobachten war. Erstmals erhielten wir mehr Eingaben im Bereich der Wirtschaft als im Bereich der Verwaltung. Diese Entwicklung spiegelt die zunehmende Bedeutung der Verarbeitung von Kundendaten in der Privatwirtschaft und zugleich das wachsende Datenschutzbewusstsein der Menschen in diesem Bereich. Kein Unternehmen kann es sich heutzutage noch leisten, Fragen des Datenschutzes als zweitrangig zu behandeln. Denn im Gegensatz zu Behörden hat es für Unternehmen oft direkte wirtschaftliche Konsequenzen, wenn bei ihnen Mängel der Datensicherheit oder nicht gesetzeskonforme Datenverarbeitungspraktiken publik werden. Um kein Missverständnis aufkommen zu lassen: Die staatliche Datenverarbeitung wird keineswegs belanglos. Aber die Datenmacht der Unternehmen hat mittlerweile mindestens so weitreichende Folgen für die Entfaltungschancen des Einzelnen wie die Datenverarbeitungssysteme der Eingriffs- und Leistungsverwaltung.

7.3 Zusammenarbeit mit dem Abgeordnetenhaus

Der Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses hat im vergangenen Jahr neben der Stellungnahme des Senats zum Jahresbericht 2004 zahlreiche aktuelle Fragen des Datenschutzes und der Informationsfreiheit erörtert. Dabei haben die Mitglieder des Unterausschusses mehrfach die Position des Berliner Beauftragten für Datenschutz und Informationsfreiheit fraktionsübergeifend unterstützt. Die Entschließungen des Unterausschusses zum Jahresbericht 2003 wurden vom Abgeordnetenhaus in der Sitzung am 17. März 2005 beschlossen.

7.4 Zusammenarbeit mit anderen Stellen

Ohne die enge Kooperation mit anderen Datenschutzaufsichtsbehörden und Beauftragten für Informationsfreiheit wären kaum sichtbare Erfolge bei der Durchsetzung von mehr Selbstbestimmung und Transparenz in der Informationsgesellschaft zu erzielen.

Deshalb war die Zusammenarbeit in der *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, die im vergangenen Jahr unter dem Vorsitz des Leiters des Unabhängigen Landeszentrums Schleswig-Holstein tagte, von besonderer Bedeutung. Im Laufe des vergangenen Jahres, insbesondere bei ihren Sitzungen am 11./12. März 2005 in Kiel und am 27./28. Oktober 2005 in Lübeck fasste die Konferenz zahlreiche Entschließungen zu

grundlegenden Fragen des Datenschutzes, die auch für Berlin von Bedeutung sind[141]. Auch an den zahlreichen Arbeitskreisen der Datenschutzkonferenz beteiligten wir uns. Darunter ist auch der neu gebildete Arbeitskreis zu Fragen des „Datenschutzgerechten eGovernment“ zu nennen, der sich sowohl mit der Ausgestaltung von Basiskomponenten wie z.B. dem Dokumenten-Management, der Archivierung und den Verzeichnisdiensten, aber auch mit Fachverfahren wie dem elektronischen Meldeverfahren befasst.

Die gute Zusammenarbeit mit Brandenburg wurde auch nach der Wahl von Frau Dagmar Hartge, der bisherigen Leiterin des Bereichs Recht in unserer Dienststelle, zur neuen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht fortgesetzt. Unabhängig vom Fortgang der Debatte über eine mögliche Fusion der beiden Länder sollte alles dafür getan werden, um so viele Kräfte der beiden Behörden wie möglich zu bündeln. Dadurch kann die Beratung und Kontrolle von Datenverarbeitern im Interesse der Bürgerinnen und Bürger in Berlin und Brandenburg noch effektiver gestaltet werden.

Wir beteiligten uns an den beiden Sitzungen des „Düsseldorfer Kreises“ in Potsdam, dem Koordinierungsgremium der Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 21./22.4. und 10./11.11.2005, das im vergangenen Jahr turnusmäßig unter dem Vorsitz des brandenburgischen Ministeriums des Innern tagte. Außerdem nahmen wir an den Sitzungen der Arbeitsgruppen dieses Gremiums teil. Die Arbeitsgruppen „Internationaler Datenverkehr“ und „Telekommunikation, Tele- und Mediendienste“[142] werden von uns betreut.

Die *Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland*, an der die Landesbeauftragten (ab 2006 auch der Bundesbeauftragte) für Informationsfreiheit teilnehmen, tagte im vergangenen Jahr am 27. Mai in Potsdam und am 14. November in Düsseldorf. Dabei standen die Beratungen zum neuen Bundesinformationsfreiheitsgesetz, die Transparenz in öffentlichen Unternehmen und die Offenlegung von Aktivitäten und Bezügen der Mitglieder öffentlicher Organe und Gremien im Vordergrund[143]. Bei einer Anhörung des Bundestagsinnenausschusses zum Entwurf des Bundesinformationsfreiheitsgesetzes hat die Arbeitsgemeinschaft eine gemeinsame Stellungnahme abgegeben, die in Teilen auch zu Verbesserungen des Entwurfs führte.

Traditionell vertritt der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Aufsichtsbehörden der Bundesländer in der *Arbeitsgruppe nach Art. 29* der Europäischen

141 vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2005“, S. 11 ff.
142 vgl. 5.1
143 vgl. Anlagenband, a.a.O., S. 116 ff.

Datenschutzrichtlinie[144]. Die *Europäische Datenschutzkonferenz* fand am 26./27. April in Krakau statt[145]. Wir berichteten dort über unsere Koordinierungstätigkeit im Bereich des grenzüberschreitenden Datenverkehrs und der bindenden Unternehmensregelungen. Die Internationale Konferenz der Datenschutzbeauftragten verabschiedete am 16. September 2005 in Montreux eine Erklärung zum universellen Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt (Erklärung von Montreux) sowie Entschließungen zur Verwendung der Biometrie in Pässen und zur Wahlwerbung[146].

Unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit tagte die inzwischen weltweit als *„Berlin Group“* bekannte *Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation* am 31. März/1. April 2005 in Funchal/Madeira und am 6./7. September 2005 in Berlin. Sie befasste sich mit Themen wie den Datenschutzrisiken bei Online-Wahlen, des Web Browser Caching und der netzwerkbasierten Telemedizin[147]. Der Vorsitzende der Internationalen Arbeitsgruppe hat deren Standpunkt bei einer Konferenz der Internationalen Fernmeldeunion am 1. Juli 2005 in Genf zur Vorbereitung des Weltgipfels zur Informationsgesellschaft (2. Phase) erläutert.

Die auf Initiative des Berliner Beauftragten für Informationsfreiheit gegründete *Internationale Konferenz der Informationsfreiheitsbeauftragten* hielt ihre 3. Sitzung vom 20.–23. Februar 2005 auf Einladung der mexikanischen Informationszugangskommission in Cancún ab.

7.5 Europäische Akademie für Informationsfreiheit und Datenschutz

Die bewährte Zusammenarbeit mit der Europäischen Akademie für Informationsfreiheit und Datenschutz wurde im vergangenen Jahr fortgesetzt. Gemeinsam mit der Akademie wurden wieder drei Veranstaltungen durchgeführt:

Am 7. April 2005 fand ein Workshop zu „Informationsfreiheit, Pressefreiheit und Datenschutz“ statt, an der auch der Europäische Datenschutzbeauftragte Peter Hustinx teilnahm. Ein Workshop zu dem immer wichtiger werdenden Thema „Überwachung am Arbeitsplatz“ schloss sich am 17. Juni 2005 an. Schließlich trafen sich am 24./25. November 2005 Informationsfreiheitsbeauftragte aus Europa und gründeten die *Europäische Konferenz der Informationsfreiheitsbeauftragten*[148].

144 vgl. Anlagenband, a.a.O., S. 33 ff.
145 vgl. Anlagenband, a.a.O., S. 27 ff.
146 vgl. Anlagenband, a.a.O., S. 95 ff.
147 vgl. Anlagenband, a.a.O., S. 106 ff.
148 vgl. Anlagenband, a.a.O., S. 118

7.6 Öffentlichkeitsarbeit

Um die Sichtbarkeit des Datenschutzes und der Informationsfreiheit in Berlin zu erhöhen, beteiligten wir uns im vergangenen Jahr an einer Reihe öffentlicher Veranstaltungen:

- 34. Tag der offenen Tür der Berliner Polizei 2005 am 22. Mai 2005
- Tag der offenen Tür des Abgeordnetenhauses von Berlin am 4. Juni 2005
- Langen Nacht der Wissenschaften am 11. Juni 2005
- Jugendverbraucherschutztag am 28. September 2005.

Wir werden uns auch künftig an entsprechenden Veranstaltungen beteiligen, um Bürgerinnen und Bürger über den Datenschutz und die Informationsfreiheit zu informieren und uns ihren Fragen zu stellen. Gerade der altersgerechten Information von Jugendlichen, aber auch von Senioren messen wir große Bedeutung bei.

Berlin, den 29. März 2006
Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit