Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Datenschutz und Informationsfreiheit

Bericht 2011

Berlin

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2011

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am **30. März 2011** vorgelegten Jahresbericht 2010 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2011 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2011“) veröffentlicht.

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: (030) + 138 89-0
Telefax: (030) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Satz: LayoutManufaktur.com

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Inhaltsverzeichnis

5. Justiz

6. Finanzen

7. Sozialordnung

Einleitung

Jede Datenverarbeitung ist riskant. Dass die Risiken gerade bei der Verarbeitung personenbezogener Daten dramatisch zunehmen, wurde im zurückliegenden Jahr deutlicher als je zuvor. Wer das Internet nutzt, kann bequem vom heimischen Computer aus Bücher bestellen, Reisen buchen und sich neuerdings auch zunehmend Behördengänge ersparen, wenn entsprechende E-Government-Dienste angeboten werden. Nach bisherigem Kenntnisstand konnte die Nutzung solcher Angebote mit dem Verschlüsselungsverfahren „Secure Socket Layer (SSL)“ hinreichend abgesichert werden. Im September wurde erstmals ein Anbieter der dafür nötigen Zertifikate, das niederländische Unternehmen **DigiNotar,** Opfer eines groß angelegten Hackerangriffs. Aufgrund des Angriffs wurden über 500 Zertifikate gefälscht, die ihrerseits zur Fälschung von Webseiten genutzt werden können. DigiNotar war kein beliebiger Anbieter, sondern als Dienstleister für Notare und die niederländische Regierung im Rahmen der staatlichen Verschlüsselungsinfrastruktur tätig. DigiNotar stellte den gesamten elektronischen Kontakt der niederländischen Bevölkerung zu ihrer Regierung sicher und musste aufgrund des Vorfalls Insolvenz anmelden. Ein anderes niederländisches Unternehmen, zu dem die Kunden von DigiNotar wechselten, musste ebenfalls aufgrund von Sicherheitsproblemen für zwei Wochen seine Online-Dienste einstellen.

Dieser Vorfall ist deshalb bedrohlich, weil nicht nur in den Niederlanden, sondern auch in Deutschland und Berlin die Vertrauenswürdigkeit von elektronischen Dienstleistungen und der Schutz der dabei erhobenen personenbezogenen Daten wesentlich von einer Technik abhängen, die auf sicheren Zertifikaten beruht. Der Fall DigiNotar ist deshalb bereits als GAU (größter anzunehmender Unfall) bezeichnet worden und das mit Recht. Wir vertrauen um der Bequemlichkeit willen immer mehr Daten auf elektronischem Weg Unternehmen und Behörden an, ohne darüber nachzudenken, ob dieser Transportweg oder die Verarbeitung der Daten beim Empfänger sicher ist. Wer die moderne Technik nutzt, ist in aller Regel auch gar nicht in der Lage, die Sicherheit dieser Technik zu kontrollieren. Er muss sich auf Unternehmen verlassen, die – wie DigiNotar – Sicherheit als Dienstleistung anbieten. Wenn solche Sicherheitsdienste kompromittiert werden, droht eine ganze Infra-

struktur der Kommunikation zusammenzubrechen. Der Angriff auf DigiNotar war zudem kein Einzelfall, sondern reihte sich ein in eine Kette spektakulärer Sicherheitsverletzungen im zurückliegenden Jahr[1], die teilweise auf kriminelle Hackerangriffe, sehr häufig aber auch auf eine sträfliche Vernachlässigung der Datensicherheit durch die verantwortlichen Regierungen und Unternehmen zurückzuführen waren.

Allerdings ist Datensicherheit nicht alles. Auch die sichere Verarbeitung von personenbezogenen Daten birgt gravierende Risiken, wenn sie exzessiv betrieben wird. Solche Arten der Datenverarbeitung gefährden den Freiheitshaushalt einer Demokratie. Deshalb gehört es zu den positiven Nachrichten des zurückliegenden Jahres, dass das **ELENA-Verfahren** eingestellt wurde, das eine zentrale Speicherung von Beschäftigtendaten auf Vorrat vorsah. Das entsprechende Bundesgesetz hätte vor dem Bundesverfassungsgericht voraussichtlich keinen Bestand gehabt[2] und wurde deshalb im Oktober aufgehoben[3]. Diese Entscheidung des Bundesgesetzgebers entband zugleich den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der sachfremden Aufgabe, den Datenbankhauptschlüssel für dieses Verfahren zu verwahren. Seit Dezember nahm die zentrale Speicherstelle keine Meldungen der Arbeitgeber für das ELENA-Verfahren mehr an. Bis Ende Februar 2012 sollen sämtliche angefallenen personenbezogenen Daten gelöscht sein. Sollte der Bundesgesetzgeber ein neues Verfahren für elektronische Entgeltnachweise auf den Weg bringen, so muss er von einer zentralen Speicherung auf Vorrat absehen und sollte lediglich anlassbezogen die elektronische Erstellung solcher Nachweise vorsehen.

In einer Zeit, in der große US-Unternehmen wie **Google, Facebook, Apple und Amazon** immer größere Sammlungen von Nutzerdaten anlegen, ohne bisher das europäische und deutsche Datenschutzrecht ausreichend zu berücksichtigen, steht der Datenschutz vor einer besonderen Herausforderung[4]. Er muss einerseits darauf dringen, dass diese monopolähnlichen Unternehmen das Recht des Landes respektieren, in dem sie ihre Dienste anbieten. Deshalb ist

1 Siehe 1.2.2
2 Siehe JB 2010, Einleitung
3 Gesetz zur Änderung des Beherbergungsstatistikgesetzes und des Handelsstatistikgesetzes sowie zur Aufhebung von Vorschriften zum Verfahren des elektronischen Entgeltnachweises, BGBl. I, S. 2298
4 Siehe dazu 12.2, 15.1

es sehr zu begrüßen, dass der europäische Gesetzgeber diesem Grundsatz jetzt Geltung verschaffen will. Andererseits ist **Berlin „stolz auf seine florierende digitale Gründerszene“**[5]. Auch die in dieser Szene immer zahlreicher entstehenden Start-up-Unternehmen erwarten Beratung und Unterstützung vom Datenschutzbeauftragten. Zunehmend machen sie Datenschutz zum Qualitätsmerkmal ihres Geschäftsmodells, was positiv ist. Allerdings sollte auch Datenschutz „drin sein“, wo Datenschutz „draufsteht“. Dann kann Datenschutz zum Wettbewerbsvorteil werden.

Die Gesetze zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz) und zur Förderung der Informationsfreiheit im Land Berlin (Berliner Informationsfreiheitsgesetz) finden allein Anwendung auf die Behörden und sonstigen öffentlichen Stellen des Landes. Für das **Abgeordnetenhaus von Berlin** gelten sie nur, soweit die Verwaltung des Parlaments betroffen ist. Die parlamentarische Tätigkeit unterliegt weder dem Datenschutzgesetz noch dem Informationsfreiheitsgesetz, insbesondere hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit in diesem Bereich keine Kontrollbefugnisse. Allerdings gehört es zu seinen Aufgaben, die Auswirkungen der automatischen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der Behörden und sonstigen öffentlichen Stellen dahingehend zu beobachten, ob sie zu einer Beschränkung der Kontrollmöglichkeiten durch das Abgeordnetenhaus oder die Bezirksverordnetenversammlungen führen. Er kann Maßnahmen zum Schutz gegen derartige Auswirkungen anregen.[6]

Seit längerem setzt sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit dafür ein, dass das Abgeordnetenhaus für den parlamentarischen Bereich Regelungen zum Umgang mit personenbezogenen Daten trifft und eine interne Kontrolle z.B. durch einen Ausschuss vorsieht. Eine solche Regelung würde den Datenschutz über die bereits bestehende Geheimschutzordnung hinaus umfassend gewährleisten. Das Abgeordnetenhaus würde zudem dem Beispiel anderer Landesparlamente[7] folgen, die derartige Regelungen bereits erlassen haben.

5 So die Süddeutsche Zeitung vom 1. Februar 2012, S. 6
6 § 24 Abs. 3 BlnDSG
7 Z. B. in Hamburg, Hessen, Rheinland-Pfalz und Schleswig-Holstein

Auch die Frage, inwieweit Bürgerinnen und Bürger ein Recht auf Informationszugang gegenüber dem Abgeordnetenhaus haben, ist nicht hinreichend geklärt. Zweifelsfrei gilt das Informationsfreiheitsgesetz für die Parlamentsverwaltung, nicht aber für den parlamentarischen Bereich. Die Abgrenzung zwischen der Verwaltungstätigkeit und der parlamentarischen Arbeit bereitet allerdings immer wieder Schwierigkeiten. So hat das Verwaltungsgericht Berlin einem Bürger das Recht auf Einsicht in ein Gutachten des Wissenschaftlichen Dienstes des Deutschen Bundestages zur Existenz von Unbekannten Flugobjekten (UFOs) zugesprochen.[8] Es erscheint in der Tat wenig sachgerecht, solche Gutachten generell vom Anwendungsbereich des Informationsfreiheitsrechts auszunehmen. Unabhängig davon sollte das Abgeordnetenhaus auch die Frage aufgreifen, inwieweit das Informationsfreiheitsrecht im parlamentarischen Raum in bestimmten Grenzen gelten sollte. Es wäre deshalb zu begrüßen, wenn die Fraktionen des Abgeordnetenhauses den Gedanken eines **Parlamentsinformationsgesetzes** aufgreifen würden, in dem sowohl Fragen des Datenschutzes als auch der Informationsfreiheit im parlamentarischen Raum (wie die Zulässigkeit von Livestreams[9]) geregelt werden könnten. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit würde ein solches Vorhaben beratend begleiten.

8 Urteil vom 1. Dezember 2011, Az.: 2 K 91.11 – nicht rechtskräftig
9 Vgl. 13.2. in Bezug auf „Bezirksparlamente“ (BVV)

1. Technische Rahmenbedingungen

1.1 Entwicklung der Informationstechnik

Die Verwendung von Informations- und Kommunikationstechnik zur Beschneidung der Persönlichkeitsrechte

Als George Orwell 1948 seinen Roman „1984“ schrieb, war der Computer bereits erfunden. ENIAC[10], eine fabrikhallengroße Apparatur, bestückt mit Tausenden von Elektronenröhren, gilt als erster elektronischer Universalrechner. Mit ihm wurden ballistische Tabellen für die US-Armee berechnet. Andere – noch nicht universelle – Computer (Colossus) dienten den britischen Streitkräften bei der Entschlüsselung verschlüsselter Nachrichten der deutschen Wehrmacht. Ob Orwell von diesen Entwicklungen gewusst hat, ergibt sich aus seinem Roman nicht. Die totale Überwachung durch den „Big Brother“, der Gedankenpolizei der Potentaten in Orwells Szenario, erfolgte nicht mithilfe von Computern, sondern durch „Teleschirme“[11], die sowohl der Darstellung als auch der Aufnahme von Bildern dienten, je nachdem, ob Propaganda zu verbreiten oder die Untertanen zu beobachten waren. Darüber hinaus sollten Mikrofone und Hubschrauber den Menschen klarmachen, dass sie einer ständigen Überwachung ausgesetzt waren und jedes unerwünschte Verhalten seine Ahndung zur Folge haben könnte.

Sicher ist wohl, dass Orwell beim Teleschirm noch nicht an PCs oder Notebooks mit Internetverbindung und Webcams und bei den Hubschraubern an Drohnen gedacht hat. Sicher ist aber auch, dass diese modernen Techniken heute zur (heimlichen) Beobachtung von Menschen ge- bzw. missbraucht werden. Das Repertoire von Orwells „Big Brother“ bei der informationellen Unterdrückung findet heute aufgrund der technischen Entwicklung zwar seine Entsprechung, jedoch ahnte Orwell noch nicht, dass 60 Jahre später über den Teleschirm, das Mikrofon und den Hubschrauber hinaus das Arsenal zur technischen Überwachung menschlicher Lebensäußerungen wesentlich erweitert

10 Electronic Numerical Integrator and Computer

11 In älteren Übersetzungen des Romans ist von „Televisoren“ die Rede.

und ein Ende der Entwicklung nicht abzusehen sein würde. Die Beobachtung der Entwicklung der modernen Informations- und Kommunikationstechnik (IKT) wäre unvollständig, würde man dabei nicht auch die Entwicklung der Kontroll- und Überwachungstechnik im Auge haben. Dabei kann man von einer „dual use"-Technik sprechen, derer sich Demokratien bedienen, die sich der Kriminalität und antidemokratischer Unterwanderung erwehren, aber auch Diktaturen, die demokratische Bestrebungen unterdrücken. Wir leben nicht in einer orwellschen Überwachungsdiktatur. Aber Orwells Vision darf auch nicht als legitimierende Beruhigungspille herangezogen werden, die uns suggerieren soll: „So schlimm ist es ja (noch) nicht."

Überwachungstechnik zur Beobachtung menschlichen Handelns begegnet uns in den Städten allgegenwärtig in Form der **Videoüberwachung**, meist verbunden mit der Aufzeichnung der aufgenommenen Bilder. Die Polizeibehörden dürfen Videoüberwachung betreiben im Rahmen der Befugnisse, die ihnen die Polizeigesetze[12] zugestehen. Dies ist in den Bundesländern unterschiedlich, jedoch setzt die polizeiliche Videoüberwachung in der Regel voraus, dass nach allgemeiner Erfahrung oder nach den Umständen des Einzelfalls die Annahme gerechtfertigt ist, dass im beobachteten Bereich im Beobachtungszeitraum Straftaten begangen werden. Im Verhältnis zu der Videoüberwachung, die in den Datenschutzgesetzen des Bundes und der Länder geregelt ist, sind die Befugnisse der Polizei eher restriktiv geregelt.

Die Videoüberwachung durch andere Behörden und Private ist nach den Datenschutzgesetzen möglich, wenn sie für die Wahrnehmung öffentlicher Aufgaben oder des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der beobachteten Personen entgegenstehen. Es sind also Abwägungen zwischen zwei Interessenlagen erforderlich, die bei den Überwachungswilligen in vielen Fällen von vornherein zugunsten der Überwachung ausfallen. Die Videoüberwachung in Einkaufszentren, Ladengeschäften und Tankstellen, in den Außen- und Innenbereichen von Wohnanlagen, Büro- und Geschäftsgebäuden, der Außenfassaden von Gebäuden, in öffentlichen Verkehrsmitteln und sogar hinsichtlich der Privatsphäre besonders sensitiven Berei-

12 In Berlin das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG)

chen[13] ist auch in Berlin gelebter Alltag. Da Videokameras für kleines Geld mittlerweile in Baumärkten erworben werden können, müssen die Datenschutzbehörden häufig Privatleute davon überzeugen, dass es nicht der öffentlichen Sicherheit oder dem Hausrecht dient, wenn sie den Garten oder die Haustür der Nachbarschaft beobachten oder mit der Beobachtung des Bürgersteigs oder des Parkplatzes auf der Straße Befugnisse ausgeübt werden, die nicht einmal der Berliner Polizei zugestanden werden. Videoüberwachung pervertiert zum „Volkssport".

In Verbindung mit der biometrischen **Gesichtserkennung** kann die Videotechnik zu einem Instrument zur Überwachung von bestimmten Personen werden. Bisherige Versuche – z.B. auf dem Hauptbahnhof in Mainz im Jahre 2007 – sind zwar gescheitert, aber es steht zu erwarten, dass sich die Technik soweit verbessern wird, dass sie zunächst die Identifizierung sich kooperativ verhaltener Personen möglich machen wird und später auch bei der Personenfahndung wirksam werden kann. Die Software für einen zweiten „Volkssport" ist bereits auf dem Markt.[14] Facebook und Google+ spielen die Vorreiter.

Eine weitere Form der direkten Personenbeobachtung deutet sich mit der **Überwachung aus der Luft** an. Mit der Entwicklung hochauflösender Kamerasysteme, die von Flugkörpern wie z.B. tiefffliegenden **Drohnen**[15] aus betrieben werden, wird aus der militärischen Luftaufklärung aus Flugzeugen ein System zur Identifizierung und Beobachtung von Personen. Auch im privaten Bereich gibt es für die UAS (Unmanned Aerial Systems) – wie die Geräte in einem Gesetzgebungsvorhaben der Bundesregierung genannt werden[16], um den militärischen Bezug zu vermeiden – ein steigendes Interesse. Bei Preisen ab 250 Euro kann man so die Beobachtung der Nachbarschaft optimieren.[17] Luftbilddienste wie Google Earth ermöglichen zwar bisher noch nicht die Identifizierung von Personen, aber die Aufnahmetechnik dafür dürfte bald verfügbar sein.

13 Vgl. 2.4

14 Vgl. http://www.heise.de/thema/Gesichtserkennung

15 „Über Deutschland sollen schwere Drohnen fliegen", WELT-ONLINE vom 28. Dezember 2011

16 Entwurf eines Vierzehnten Gesetzes zur Änderung des Luftverkehrsgesetzes, BT-Drs. 17/8098

17 Süddeutsche Zeitung vom 30. Dezember 2011, S. 4: „Der gefilmte Bürger", S. 5: „Drohnen gegen Kriminelle"

Die Persönlichkeitsrechte der Betroffenen werden nicht nur tangiert, wenn sie selbst beobachtet werden. Ebenso wird in die Persönlichkeitsrechte durch Überwachung eingegriffen, wenn ihr Verhalten beim Konsum, bei der Kommunikation und bei der tagtäglichen Besorgung ihrer Angelegenheiten verdeckt registriert wird. Bereits jetzt haben die **RFID-Chips**[18] eine erhebliche Verbreitung erlangt. Zunächst als Verbesserung der Barcode-Anwendungen in der Logistik eingeführt, gibt es mittlerweile eine Vielzahl von Anwendungen in allen Lebensbereichen. Elektronische Reisepässe und Personalausweise sind längst mit diesen Chips ausgestattet, die eine Auslesung und Speicherung ohne Kontaktschnittstellen ermöglichen. Nachdem bereits bei der Fußball-Weltmeisterschaft 2006 die Eintrittskarten mit RFID-Chip ausgestattet waren, werden heute vielfach bei bedeutenden Konzerten die Karten ebenfalls mit RFID-Chip personalisiert, um den Schwarzmarkt zu unterbinden. Da die RFID-Chips je nach Bauart kürzere oder längere Reichweiten haben, variiert auch die Gefahr des unbefugten Auslesens von Daten. RFID-Chips mit Reichweiten von mehreren Metern können aus unverdächtiger Entfernung heimlich ausgelesen werden, sofern ein Lesegerät eingesetzt wird, das zu den Chips kompatibel ist. Dagegen sind Sicherheitsmaßnahmen möglich (Authentifizierung von Lesegeräten, Verschlüsselung des Chipinhaltes), wenn die beobachtende Stelle nicht mit dem Herausgeber der Chips zusammenarbeitet.

Mit der Weiterentwicklung der RFID-Technologie erfolgt eine fortschreitende Miniaturisierung der elektronischen Bausteine. Mikroprozessoren, Sender, Empfänger, Sensoren und Aktoren können nach Auffassung namhafter Fachleute Netze aus **„intelligentem Staub“** (smart dust) bilden. Allgegenwärtiger (ubiquitous) oder umsichgreifender (pervasive) Rechnereinsatz führt zum **„Internet der Dinge“**[19] mit der Möglichkeit, unauffällig, effizient und billig die in diesem Netz handelnden Menschen zu überwachen.

Der aufschlussreichste Ansatz zur Überwachung von Personen und zur Gewinnung von aussagefähigen Profilen ist die **Beobachtung ihrer Kommunikation.** Der sog. „Große Lauschangriff“ zielt auf das gesprochene Wort in privaten Räumen, also der akustischen Wohnraumüberwachung zu Zwecken der Straf-

18 Radio Frequency Identification; vgl. JB 2004, 3.4; JB 2005, 2.1

19 Fleisch, E.; Mattern, F. (Hrsg.): Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis, Berlin 2005; vgl. auch 12.7

verfolgung. Dieser Eingriff in die Unverletzlichkeit der Wohnung, der in den meisten Fällen auch vorbereitende Maßnahmen in der Wohnung voraussetzt, ist nur bei der Verfolgung schwerster Verbrechen auf Anordnung einer Staatsschutzkammer gerechtfertigt. Er muss nach der Rechtsprechung des Bundesverfassungsgerichts[20] unterbleiben oder ggf. abgebrochen werden, wenn der Kernbereich persönlicher Lebensgestaltung durch den Eingriff verletzt werden kann.

Die **Telekommunikationsüberwachung**, also das Mithören und Mitschneiden von Telefonaten, das Mitlesen von E-Mails, SMS und Telefaxsendungen ist in Form der Telefonüberwachung eine der ältesten auf technischer Überwachung beruhenden Ermittlungsformen bei der Strafverfolgung. Auch sie bedarf der Anordnung eines Richters, bei Gefahr im Verzug eines Staatsanwalts. Die Betreiber solcher Telekommunikationsdienste haben technische Schnittstellen bereitzuhalten, die den Strafverfolgungsbehörden die Telekommunikationsüberwachung ermöglichen.

Eine neue Dimension enthält die **Überwachung der Internet-Telefonie**[21], meist unter Verwendung des Skype-Dienstes. Da diese Telefongespräche als digitale Zeichenketten übertragen werden, erfolgt die Kommunikation mit einer leistungsstarken Verschlüsselung. Diese Ver- und Entschlüsselung findet an den Kommunikationsendpunkten statt, also unmittelbar bei den Teilnehmern. Eine Überwachung dieser Telefonate ist daher nur möglich, wenn sie unmittelbar an den als Endgerät dienenden Computern erfolgt, bevor die Verschlüsselung vorgenommen wurde oder – beim Empfänger – nachdem die Entschlüsselung stattfand. Diese sog. **Quellen-Telekommunikationsüberwachung** setzt also die Manipulation eines der beteiligten Computer voraus. Dazu bedienen sich die Strafverfolgungsbehörden einer Methode, die zuvor eher bei der Begehung von Computerstraftaten angewandt wurde: Sie schleusen eine Schadsoftware ein, die den Computer veranlasst, etwas für den Nutzer Schädliches zu tun, in diesem Fall vor der Verschlüsselung das VoiP-Gespräch aufzuzeichnen und den Inhalt an Server der Behörden zu übertragen.

20 1 BvR 2378/98; BVerfGE 109, 279 ff.

21 Voice over Internet-Protocol (VoiP)

Der Chaos Computer Club (CCC), dem Kopien eines solchen Programms zugespielt worden waren, stellte fest, dass diese **„Staatstrojaner"-Software** mit einer Nachladefunktion ausgestattet ist, die es erlaubt, bei Bedarf zusätzlichen Code nachzuladen und den Inhalt der Festplatte zu verändern. Ob diese vorgesehene Funktion auch erlaubt, manipulativ Scheinbeweise für kriminelles Handeln in den angegriffenen Computer zu laden, blieb offen. Bedenklich war die Feststellung des CCC, dass die Software sicherheitsrelevante Fehler aufwies, die dazu hätte führen können, dass die Schadsoftware nicht nur für staatliche Überwachungszwecke dienen, sondern auch von Kriminellen nutzbar gemacht werden könnte.[22] Zwar hat das Bundesverfassungsgericht festgestellt, dass die **Online-Durchsuchung** von Computerfestplatten mit vergleichbaren Mitteln unter Beachtung bestimmter Verfahrensregelungen verfassungsgemäß sein kann. Es hat aber gleichzeitig das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"[23] aus dem Grundgesetz abgeleitet, an dem Online-Durchsuchungen zu messen sind. Die Online-Durchsuchung greift deshalb noch einschneidender in Grundrechte ein als die Quellen-Telekommunikationsüberwachung, weil auch private Notizen, Tagebuchaufzeichnungen oder Bilder des Computer-Nutzers heimlich ausgelesen werden. Dem Bundeskriminalamt wurde die gesetzliche Befugnis zur Online-Durchsuchung in § 20k BKA-Gesetz eingeräumt. Ob diese Vorschrift verfassungskonform ist, prüft gegenwärtig das Bundesverfassungsgericht. Die vom Chaos Computer Club aufgedeckte „Staatstrojaner"-Software bestätigt unsere 2007[24] ausgesprochene Warnung, dass die Legalisierung der Online-Durchsuchung das Vertrauen der Gesellschaft in die Sicherheit unserer IT-Struktur nachhaltig erschüttern wird. Es ist schwer vorstellbar, dass die vom Bundesverfassungsgericht gezogene Grenze zwischen Quellen-Telekommunikationsüberwachung und Online-Durchsuchung in der Praxis berücksichtigt wird.

Ein weiteres Potenzial zur Überwachung von Personen ergibt sich, wenn es nicht auf ihre aktuellen Handlungen ankommt, die direkt oder indirekt beobachtet werden können, sondern durch den Nachvollzug ihrer vergangenen Handlungen, die sich aus den vielfältigen **personenbezogenen Datenbeständen** in öffentlicher und privater Hand ergeben.

22 Zur Situation in Berlin vgl. 3.3
23 1 BvR 370/07; 1 BvR 595/07; BVerfGE 120, 274 ff.
24 JB 2007, 2.1

Seit 2005 gibt es in Deutschland die **LKW-Maut** für Nutzfahrzeuge ab einer bestimmten Größenordnung bei der Benutzung von Bundesautobahnen und bestimmten Bundesfernstraßen. Die automatisierte Ermittlung der Mautgebühren erfolgt mit einem Gerät im Fahrzeug[25] mittels Satellitenortung der Fahrstrecke, deren Ergebnisse mittels Mobilfunk an den Mautbetreiber Toll Collect übertragen werden. Die Kontrolle erfolgt mit den auf den Mautstrecken aufgestellten Kontrollbrücken. Dabei werden das Kennzeichen und bestimmte Fahrzeugmerkmale gelesen sowie Fotos vom Fahrzeug zur Ermittlung der Größenklasse und zum Vergleich des Kennzeichens gemacht. Mit diesen Daten kann stichprobenhaft kontrolliert werden, ob die Mautpflicht eingehalten wurde. Der Gesetzgeber hat diesem Verfahren nur unter der Bedingung zugestimmt, dass die Daten einer besonderen Zweckbindung unterliegen, also nicht für andere Zwecke – auch nicht für die Strafverfolgung – verwendet werden dürften.[26] Diese datenschutzfreundliche Regelung geriet in die Diskussion, als zumindest die Vermutung aufkam, die gespeicherten Mautdaten könnten bei der Aufklärung von Kapitalverbrechen helfen, bei denen LKW-Fahrer bei der Nutzung mautpflichtiger Strecken als Täter in Frage kamen. Dennoch hat der Bundesgesetzgeber diese Zweckbindung im Berichtszeitraum bekräftigt.

Mit der Einführung der Europa-Kennzeichen für Kraftfahrzeuge wurde durch die Gestalt bestimmter Buchstaben und Zeichen deutlich, dass sie hinsichtlich der **Kennzeichenerfassung** (Kennzeichen-Scanning) optimiert worden waren. So war es nicht überraschend, als die ersten Versuche stattfanden, die Kennzeichenerkennung im rollenden Verkehr umzusetzen. Das Ziel der Behörden war das Auffinden von gestohlenen oder aus anderen Gründen gesuchten Fahrzeugen und die Fahndung nach gesuchten Fahrzeughaltern. Die Kennzeichenerkennung bedarf in den Ländern einer gesetzlichen Grundlage, die die Zwecke festlegt, zu denen sie erfolgen darf. In Berlin fehlt eine solche gesetzliche Grundlage.[27] Diese Technik wäre geeignet, Bewegungsprofile für alle Fahrerinnen und Fahrer zu erstellen. Da die Erforderlichkeit dieser Technik selbst von Fachleuten bezweifelt wird, haben die Länder Bremen und Schleswig-Holstein auf eine entsprechende Befugnis verzichtet, nachdem das Bundesverfassungs-

25 On-Board-Unit (OBU)
26 § 7 Abs. 2 Bundesfernstraßenmautgesetz, BGBl. I 2011, S. 1378
27 Vgl. JB 2009, 3.1

gericht die bisherigen gesetzlichen Regelungen als verfassungswidrig bezeichnet hatte.[28]

Nutzt man das neue Ticketing-Verfahren Touch & Travel der Deutschen Bahn AG und ihrer Kooperationspartner[29] zur Buchung und Bezahlung von Fahrkarten per Handy, so erfolgt in kurzen Abständen eine **Handyortung**, deren Ortungspunkte zur Ermittlung der genauen Fahrstrecke gespeichert werden, sodass am Ende der Fahrt der Fahrpreis ermittelt und unter den benutzten Verkehrsunternehmen verteilt werden kann. Diese Daten werden 90 Tage lang gespeichert, um auch noch Reklamationen bearbeiten zu können. Auch diese Datenquelle wäre beim Verstoß gegen die Regeln des Datenschutzes geeignet, zu einem Bewegungsprofil Entscheidendes beizutragen.

Bei der umstrittenen **Vorratsdatenspeicherung** sollten Anbieter von Telekommunikationsdiensten verpflichtet werden, alle bei der Nutzung der öffentlichen Telekommunikationsdienste anfallenden Verbindungsdaten ohne Anlass für sechs Monate zu speichern und für den Zugriff der Strafverfolgungsbehörden vorzuhalten. Das Bundesverfassungsgericht hat 2010 die Vorratsdatenspeicherung in der betriebenen Form für unzulässig erklärt und die sofortige Löschung aller bis dahin auf Vorrat gespeicherten Daten verfügt.[30] Seither ist eine Neuregelung innerhalb der Bundesregierung umstritten. Selbst eine Vorratsdatenspeicherung, die den Anforderungen des Bundesverfassungsgerichts genügt, würde zu einem riesigen Datenbestand führen, der im Wesentlichen aus Daten unbescholtener Bürgerinnen und Bürger besteht, die im Falle des Missbrauchs zu Kommunikationsprofilen zusammengefasst und zu deren Nachteil verwendet werden können.

Das Verbraucherverhalten der Menschen wird ununterbrochen intensiv beobachtet und zu Profilen verdichtet. Verbraucherumfragen, der Einsatz von Rabatt- und Kundenkarten und die Verfolgung der Internet-Aktivitäten durch die Anbieter gewerblicher Inhalte führen dazu, dass immer mehr bekannt wird, wofür die Menschen wieviel Geld ausgeben, welche Interessen sie haben, in welchen Geschäften oder in welchen Online-Shops sie kaufen. Damit können

28 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 ff.
29 Vgl. 4.2
30 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, BVerfGE 125, 260 ff.; vgl. JB 2010, 13.1

die Menschen nicht nur bestimmten **Konsumentenprofilen** zugeordnet werden, um sie dementsprechend zu umwerben, diese Profile können sogar einzelnen Personen zugeordnet werden. Das **Verbraucherverhalten** wird individuell sichtbar, sodass die aus diesem Verhalten ableitbaren Informationen über eine Person[31] für beliebige Zwecke der Einflussnahme (insbesondere Werbung) verwendet werden können.

Welche Lebensgewohnheiten pflege ich in meinen vier Wänden? Wann dusche ich und wie lange? Koche ich mit Gas oder elektrisch? Wie bereite ich Kaffee oder Tee zu? Habe ich eine Alarmanlage oder nicht und wenn ja, wann ist sie im Betrieb? Wird der Kühlschrank häufig geöffnet? Wann und wie oft laufen Waschmaschine, Trockner oder Geschirrspülmaschine? Diese und viele andere interessante Details unserer Lebensführung[32] in der nach dem Grundgesetz unverletzlichen Wohnung könnten von außen beobachtet werden und bei Dritten Rückschlüsse bewirken, wenn die Prinzipien der Datensparsamkeit und -vermeidung und konsequente Informationssicherheit bei der sog. Energiewende nicht frühzeitig berücksichtigt werden. Elektronische Messsysteme **(Smart Meter)** für den Energieverbrauch, derzeit noch vorwiegend für den elektrischen Strom, werden in bestimmten Fällen bereits seit 2010 bei Neubauten oder umfassenden Sanierungsvorhaben aufgrund gesetzlicher Verpflichtung eingebaut[33]. Die im Viertelstundentakt ausgelesenen Stromverbrauchsdaten sollen der Nutzerin und dem Nutzer das eigene Verbrauchsverhalten bewusst machen und den Stromerzeugern das Angebot zeit- und verbrauchsabhängiger Tarife ermöglichen. Künftig werden Energie verbrauchende Geräte, Smart Meter, industrielle Energieverbraucher, Energienetzbetreiber und Energieerzeuger[34] über ein Energieinformationsnetz **(Smart Grid)** verbunden, um Energieverbrauch und Energieerzeugung durch Kostenanreize zu koordinieren und die Einschaltzeiten geeigneter Stromverbraucher in Wohnungen und in der Wirtschaft zu steuern. Natürlich können die Daten, die die Smart Meter erfassen, den gläsernen Verbraucher über **Energieverbrauchsprofile** mit dem gläser-

31 Wie Alter, finanzielle Stellung, Hobbies, Ernährungsgewohnheiten, Modebewusstsein, Vorlieben, Abneigungen u. v. a. m.

32 Das geht sogar bis zu der Feststellung der genauen Typen der genutzten Geräte.

33 Vgl. 7.4.1 und JB 2009, 1.1.1

34 Darunter auch die „Prosumer", also jene, die sowohl Strom produzieren (z.B. mittels Photovoltaik) und ins Netz speisen als auch Strom konsumieren.

nen Bewohner verknüpfen, wenn sie ohne Anonymisierung und Aggregation in das Smart Grid geleitet werden. Die Weichen dazu werden aktuell gestellt[35].

Videoüberwachung, kamerabestückte Flugkörper, das allgegenwärtige „Internet der Dinge", Netze aus „intelligentem Staub", große und kleine Lauschangriffe, Telekommunikationsüberwachung (auch per Quellen-TKÜ bei der Internet-Telefonie) und Online-Durchsuchungen stehen als moderne Überwachungsmethoden zur Verfügung. Ergänzt um die gespeicherten Bewegungs-, Telekommunikations-, Konsumenten- und Energieverbrauchsprofile als verfügbare und damit im Prinzip nutzbare Datenquellen bilden sie ein erhebliches Arsenal an Überwachungsoptionen. Ihre Nutzung zu staatlichen Zwecken, insbesondere der Strafverfolgung, mag unter Beachtung der Persönlichkeitsrechte und dem Prinzip der Verhältnismäßigkeit sowie unter den wachsamen Augen des Bundesverfassungsgerichts in einer Demokratie noch hinnehmbar sein. Da aber die reine Verfügbarkeit der Überwachungsmethoden und der Datenquellen stets Begehrlichkeiten auslöst, sie für persönlichkeitsrechtswidrige oder kriminelle Zwecke zu gebrauchen, sollten die Zurückhaltung bei der Kombination der Überwachungspotenziale und der Grundsatz der Datensparsamkeit zu den wichtigsten Prinzipien zur Wahrung der informationellen Selbstbestimmung, aber auch aller anderen Persönlichkeitsrechte gehören. Dass dies selbst in demokratischen Ländern nicht selbstverständlich ist, zeigt das Folgende:

Wer das Suchwort **„INDECT"**[36] bei der meistgenutzten Suchmaschine eingibt, erhält 240.000 Quellen genannt[37]. Auch wenn in der täglichen Presse der Begriff bisher nur selten angerissen wird, so findet man im Internet eine Vielzahl von Informationen und Meinungen zu diesem EU-Projekt. Nach Angaben der EU wird INDECT im Rahmen des 7. Forschungsrahmenprogramms finanziert. Es steht unter polnischer Federführung, läuft seit Anfang 2009, dauert fünf Jahre, kostet knapp 15 Millionen Euro und wird mit knapp 11 Millionen Euro gefördert.

35 Vgl. 7.4.1

36 Intelligent information system supporting observation, searching and detection for security of citizens in urban environment, auf Deutsch: Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Erfassung für die Sicherheit der Bürger in städtischer Umgebung

37 Stand 29. Dezember 2011

Ziele des Projekts sind die Entwicklungen[38]

- einer Plattform
  - zur Erfassung und zum Austausch operativer Daten,
  - zur Gewinnung von multimedialen Inhalten,
  - zur intelligenten Verarbeitung aller Informationen,
  - zur automatischen Erkennung von Bedrohungen,
  - zur Erkennung unnormalen Verhaltens oder von Gewalttätigkeit;
- eines Prototyps eines integrierten, vernetzten Systems zur Unterstützung der operativen Aktivitäten von Polizeibeamten und zur Bereitstellung von Techniken und Werkzeugen zur Beobachtung verschiedenartiger mobiler Objekte;
- eines neuen Typs von Suchmaschinen, die die direkte Suche von Bildern und Videos anhand von digitalen Wasserzeichen ermöglichen;
- eines Bestands an Techniken zur Beobachtung von Internetangeboten, zur Analyse der gewonnenen Informationen und zur Erkennung krimineller Aktivitäten und Bedrohungen.

Die wichtigsten Ziele des INDECT-Projekts sind

- die Testinstallation eines Überwachungssystems an verschiedenen Orten eines städtischen Ballungsraums und Erprobung eines Prototyps des Systems mit 15 Knotenpunkten,
- die Implementierung eines verteilten Computersystems, welches die Erfassung, Speicherung, nach Aufforderung effektive Verteilung und intelligente Verarbeitung von Daten ermöglicht,
- die Herstellung einer Reihe von Prototypen von Geräten für die Verfolgung mobiler Objekte,
- die Entwicklung einer Suchmaschine für die schnelle Erkennung von Personen und Dokumenten anhand von digitalen Wasserzeichen,

38 http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=1&CAT=PROJ&RCN=89374 , zuletzt aufgerufen am 29. Dezember 2011, hier in Übersetzung ins Deutsche

- die Durchführung umfassender Forschung an der digitalen Wasserzeichentechnologie für die semantische Suche im Internet,
- die Entwicklung von Agentensystemen zur ständigen und automatischen Kontrolle öffentlicher Quellen wie Webseiten, Diskussionsforen, Usenet-Gruppen, Fileservern, Peer-to-Peer-(P2P-)Netzwerke und private Computer,
- der Aufbau eines Internet-basierten intelligenten (aktiven und passiven) Datensammelsystems und der messbare Nachweis seiner Effizienz.

Mit seinem Bekanntwerden ist das Projekt INDECT von der Presse, von Politikern und natürlich von Datenschützern heftig kritisiert worden. So beschreibt „Die Zeit" das Projekt als den „Traum der EU vom Polizeistaat", in dem die Unschuldsvermutung oder der gerichtsfeste Beweis keine Rolle mehr spielen.[39] Die Westdeutsche Zeitung titelt in ihrem Online-Portal „Video-Überwachung INDECT – ‚Großer Bruder' aus Wuppertal"[40] und spricht dabei die Beteiligung der Bergischen Universität Wuppertal an dem Projekt an. Die Süddeutsche Zeitung spricht von einem „Werkzeug für Diktatoren"[41]. Der Autor beschreibt folgendes Szenario:

„Ein Mann stiehlt einer Frau die Handtasche. Doch er kommt nicht weit, eine Kamera hat ihn beobachtet und ein Computer seine Bewegungen analysiert. „Taschendieb", erkennt das System, denn er hat plötzlich die Richtung gewechselt und rennt – ein abnormales Verhalten. Die Polizei lässt Drohnen aufsteigen, die dem Dieb folgen und sein Gesicht scannen. Automatisch sucht eine Software im Internet nach weiteren Informationen und findet den Wohnort. Als er zu Hause ankommt, wartet bereits die Polizei."

Bereits 2010 hat die Piratenpartei diverse Dokumente zu INDECT veröffentlicht und das Projekt heftig kritisiert. Insbesondere hebt sie hervor, dass in

39 K. Biermann: Indect – der Traum der EU vom Polizeistaat, Zeit-Online vom 24. September 2009, http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung

40 A. Wolf: Video-Überwachung Indect – „Großer Bruder" aus Wuppertal, wz-newsline vom 15. Februar 2011, http://www.wz-newsline.de/home/panorama/video-ueberwachung-indect-grosser-bruder-aus-wuppertal-1.578701

41 Ch. Behrens: Werkzeug für Diktatoren, sueddeutsche.de, http://www.sueddeutsche.de/wissen/europaeische-ueberwachungstechnologie-werkzeug-fuer-diktatoren-1.1223440

einem Arbeitspaket des Projekts die Tatsache, dass die Polizei Gesetze und Menschenrechte respektieren muss, als Grund dafür dargestellt wird, dass die polizeilichen Methoden denen der Kriminellen hinterherhinken. Die Bedenken der Bürgerrechtler und der Datenschützer werden „eher als zu überwindendes Hindernis denn als ernstzunehmende Warnung angesehen."[42] Alexander Alvaro, innenpolitischer Sprecher der FDP im Europäischen Parlament, gehört zu den Kritikern des Projektes. Er hält das geplante Vorgehen bei der INDECT-Nutzung für „in Deutschland eindeutig verfassungswidrig" und macht darauf aufmerksam, dass nach seinem letzten Stand INDECT bereits 2012 während der Fußball-Europameisterschaft in Polen getestet werden soll.[43]

Während das INDECT-Projekt auf Überwachung von Menschen in der EU für die Sicherheit und die Strafverfolgung in den Städten zielt, bei der jedoch die Sorge um die Menschen- und Persönlichkeitsrechte ausgeblendet wird, geht das EU-Projekt **„GODIAC"**[44] noch weiter. Unter schwedischer Federführung sollen Strategien zur Handhabung politischer Proteste entwickelt werden.[45] Die Zielrichtung ist also auch das Grundrecht zur Teilnahme an friedlichen Demonstrationen.

Die Potenziale der IuK-Technik zur Überwachung menschlicher Lebensäußerungen haben Orwells Phantasie aus „1984" längst übertroffen. Informationelle Selbstbestimmung, Persönlichkeitsrechte und die sich daraus ergebenden Forderungen für die Freiheit des Einzelnen nach den Vorgaben des Grundgesetzes geraten zusehends in die Defensive gegenüber den Interessen des Staates zur Vorbeugung und Verfolgung von Straftaten und zur Gewährleistung von Sicherheit und Ordnung. Der kombinierte Einsatz von Überwachungstechniken wie bei INDECT und GODIAC treibt die Überwachungswut auf die Spitze. Es ist unter demokratischen Vorzeichen nicht nachvollziehbar, weshalb die EU für solche Projekte Steuergelder bereitstellt.

42 http://www.piratenpartei.de/100908-Piratenpartei-veroeffentlicht-INDECT-Dokumente

43 http://www.derwesten.de/politik/polen-plant-die-totale-ueberwachung-der-em-fans-id6130223.html am 4. Dezember 2011

44 Good practice for dialogue and communication as strategic principles for policing political manifestations in Europe

45 http://www.polisen.se/en/Languages/The-Swedish-Police/International-cooperation/Cooperation-in-Europe/The-Godiac-Project/

1.2 Datenverarbeitung in Berlin

1.2.1 IT-Politik

Verwaltungsmodernisierung in Berlin

Der Staatssekretärsausschuss zur Verwaltungsmodernisierung beschloss im Februar, dass 50 % der IT-Büroarbeitsplätze der Berliner Verwaltung bis 2016 mit der **elektronischen Akte** auszustatten sind. Der Senat hat die Senatsverwaltung für Inneres und Sport mit der Erarbeitung eines Umsetzungskonzeptes beauftragt. Alle Beteiligten müssen sich darüber im Klaren sein, dass es sich hierbei nicht um ein IT-, sondern in erster Linie um ein Organisationsprojekt außerordentlicher Größenordnung handelt. Dies setzt auch die Änderung von Verwaltungsregelungen voraus. Ein erster Schritt hierzu wurde gemacht, indem die Gemeinsame Geschäftsordnung für die Berliner Verwaltung[46] fortgeschrieben wurde und damit die neuen Zugangswege der Bürgerinnen und Bürger zu den Behörden und die computergestützte Weiterbearbeitung der Anliegen geregelt wurden.

Im Frühjahr lag der Referentenentwurf für ein **Berliner E-Government-Gesetz**[47] vor. Wir haben darauf hingewiesen, dass die Regelungen des Berliner Datenschutzgesetzes und weiterer spezialgesetzlicher Regelungen zum Datenschutz unberührt bleiben. Wir haben vorgeschlagen, Regelungen zum Thema „Open Data" aus dem E-Government-Gesetz in das Informationsfreiheitsgesetz zu überführen. Damit soll eine Zersplitterung der Rechtsgrundlagen beim Informationszugangsrecht verhindert werden.

Mit dem **Projekt ProDiskurs** will das Bezirksamt Marzahn-Hellersdorf die Verwaltungs- und Kommunikationskultur modernisieren. Die Bürgerinnen und Bürger werden aktiv durch eine Online-Ämterbewertung beteiligt. Ein elektronisches Bürgerterminal beschleunigt den Ämtergang, und der Aufwand für die Informationssuche für die Beschäftigten soll durch ein elektronisches Beschäftigtenportal wesentlich reduziert werden. Das Projekt wird durch den Staatssekretärsausschuss zur Verwaltungsmodernisierung gefördert,

46 Allgemeiner Teil (GGO I) vom 18. Oktober 2011, ABl. S. 2782
47 EGovG Berlin

weil es auf andere Verwaltungen übertragen werden kann und somit die Richtung der Verwaltungsmodernisierung in Berlin vorgibt. Auch die Übertragung bestimmter Forderungen des Bezirks Marzahn-Hellersdorf auf private Inkassounternehmen könnte Modellcharakter für andere Bezirke haben.[48]

Open Data

„Open Data" war ein vieldiskutiertes Thema. Es umfasst allgemein die vorhandenen Datenbestände der öffentlichen Verwaltung, die durch ihre elektronische Bereitstellung der Allgemeinheit zur Nutzung und Weiterverwendung zur Verfügung gestellt werden. Mit der Aufnahme des Open-Data-Projektes in das Senatsprogramm **„ServiceStadtBerlin"** stellt auch das Land Berlin klar, dass die Datenbestände der Verwaltung allgemein zugänglich werden sollen. Die Open Data-Initiative geht von der Grundidee aus, dass der freie Zugang zu sämtlichen Daten für jedermann möglich sein sollte, da anhand des daraus resultierenden Informationsgewinns Vorteile sowohl für den Einzelnen als auch für die gesamte Gesellschaft entstehen. Ziel ist es darüber hinaus, durch „offene Daten" mehr Transparenz im Handeln von Politik, Verwaltung, Wirtschaft und Zivilgesellschaft herzustellen und gleichzeitig dadurch Anreize zur aktiven Mitarbeit für Bürgerinnen und Bürger sowie für die Zusammenarbeit unter allen Beteiligten zu schaffen.

Als „offene Daten" werden sämtliche Datenbestände angesehen, die „im Interesse der Allgemeinheit der Gesellschaft ohne jedwede Einschränkung zur freien Nutzung, zur Weiterverbreitung und zur freien Weiterverwendung frei zugänglich gemacht werden."[49] In diesem Zusammenhang wird die Einschränkung der Nutzung von Daten durch Urheberrechte, Lizenzen, Patente und andere rechtliche Bestimmungen von einigen Vertretern der Open-Data-Bewegung kritisch gesehen. Neben Datenbeständen der öffentlichen Verwaltung können auch Daten der Privatwirtschaft, von Lehr- und Forschungseinrichtungen, Non-Profit-Organisationen, gemeinnützigen Vereinen und Medienanstalten in den Bereich von „Open Data" fallen. Beispiele hierfür sind Verkehrsinformationen, Geodaten, Statistiken, Lehrmaterial, wissenschaftliche Publikationen und Forschungsergebnisse sowie Medienbeiträge oder Untersuchungen von

48 Vgl. 6.1

49 Vgl. http://www.zeppelin-university.de/deutsch/lehrstuehle/ticc/TICC-101203-OpenGovernmentData-V1.pdf von Lucke / Geiger, S. 3

Nichtregierungsorganisationen. Neben der Forderung nach freiem Zugang zu Daten werden diese von der Open-Data-Bewegung auch in vielen Projekten selbst erzeugt und genutzt, um neue Angebote auf Basis dieser Daten zu schaffen. Beispiele hierfür sind das weltweite Projekt OpenStreetMap und darauf aufbauend das deutsche Projekt Wheelmap.org, bei dem rollstuhlgerechte Orte in Stadtpläne eingetragen werden können.

Obwohl die Idee der „offenen Daten" bereits seit den sechziger Jahren besteht, gewann sie insbesondere in den letzten Jahren zunehmend an Beachtung. Dies ist u.a. auf die von der US-Regierung unter Präsident Barack Obama gestartete Open-Government-Initiative zurückzuführen, welche auch sehr stark Elemente der Open-Data-Idee aufgreift und große Beachtung in den Medien und der Öffentlichkeit gewann. Im Rahmen dieser Initiative wurde in Kooperation mit dem indischen Open-Data-Portal India.gov.in die amerikanische Open-Data-Plattform Data.gov ins Leben gerufen.[50]

Ausgehend von der Open-Data-Bewegung im angelsächsischen Raum hat sich dieser Gedanke auch zunehmend in anderen Ländern verbreitet. In Deutschland hat Berlin im September als erstes Bundesland ein eigenes **Open-Data-Portal** unter der Adresse **daten.berlin.de** freigeschaltet. Aktuell stehen auf der Webseite 56 Datensätze[51] aus 15 unterschiedlichen Kategorien bereit[52], die zur Informationsrecherche oder auch als Basis für die Entwicklung von Smartphone-Applikationen genutzt werden können. Das Berliner Datenportal ist ein Pilot- und Testprojekt im Rahmen des Programms „ServiceStadt Berlin". Die Projektleitung hat die Senatsverwaltung für Wirtschaft, Technologie und Frauen übernommen; Projektpartner sind die Senatsverwaltung für Inneres und Sport sowie das Amt für Statistik Berlin-Brandenburg. Die Realisierung obliegt dem Fraunhofer Institut FOKUS sowie dem Portalbetreiber von Berlin.de, der BerlinOnline Stadtportal GmbH & Co. KG.[53]

50 Vgl. http://www.heise.de/open/meldung/Freie-Open-Data-Plattform-1390952.html

51 Abweichend vom normalen Gebrauch des Begriffs „Datensatz" werden hier zusammenhängende Datenbestände so bezeichnet.

52 U. a. Arbeitsmarkt, Stadtplanung, Tourismus, Wirtschaft, Öffentliche Verwaltung, Verbraucherschutz, Demographie, Bildung

53 Vgl. http://daten.berlin.de/

Die auf dem Portal bereitstehenden Daten sind auch Basis für die Berliner Beiträge zum bundesweiten Open-Data-Wettbewerb **„Apps4Deutschland“** (www.apps4deutschland.de), der im Rahmen der Messe „Moderner Staat“ von Bundesinnenminister Friedrich im November eröffnet wurde. Hierbei sind Entwickler dazu aufgerufen, Ideen für neue mobile Anwendungen vorzuschlagen oder bereits funktionsfähige Anwendungen mittels der Datenbestände der öffentlichen Hand zu entwickeln und für den Wettbewerb einzureichen. Um die Nutzung der Berliner Datensätze anzuregen, wurden drei Sonderpreise gestiftet:

- Beste App-Idee mit einem Berliner Datensatz, Stifter: init AG Berlin (Entwicklerunterstützung)
- Beste App-Anwendung mit einem Berliner Datensatz, Stifter: ITDZ Berlin (Tablet-PC)
- Beste App für Kultur und Bildung, Stifter: 3pointconcepts GmbH Berlin (Entwicklerunterstützung)

Wir begrüßen die Open-Data-Initiative als willkommenen Beitrag zur Informationsfreiheit und haben sie bei verschiedenen Veranstaltungen offen unterstützt. Selbstverständlich muss bei der Bereitstellung von Datenbeständen über eine Open-Data-Plattform streng darauf geachtet werden, dass keine personenbezogenen Daten, die nicht für die Öffentlichkeit bestimmt sind, in diesen Beständen auftreten. Auch sollte ein Kriterium für die Vergabe der Berliner Sonderpreise die Berücksichtigung des Grundsatzes „Privacy by Default“ schon bei der Gestaltung der Apps sein.[54]

Aus Sicht der Informationsfreiheit ist das Berliner Open-Data-Portal zu begrüßen, da es interessierten Bürgerinnen und Bürgern ebenso wie der Wirtschaft und freien Entwicklern den Zugang zu Informationen aus den Datenbeständen der öffentlichen Hand bietet, mit denen neue mobile Anwendungen entwickelt und offene Fragen der Menschen geklärt werden können. Aus Sicht des Datenschutzes ist es erfreulich, dass Menschen und Unternehmen eine Plattform geboten wird, über die Daten ohne Personenbezug online abgerufen werden können.

54 Vgl. JB 2010, 2.5

Demokratie Online

Zunehmend wird gefordert, die Öffentlichkeit an Meinungsbildungsprozessen direkter zu beteiligen als dies bisher in der parlamentarischen Demokratie durch turnusmäßige Wahlen von Parteien erfolgt. Eine Möglichkeit der Beteiligung der Menschen oder auch der Mitglieder von Organisationen oder Parteien an Meinungsbildungsprozessen sind Online-Plattformen wie **„Adhocracy“**[55] und **„Liquid Feedback“**, bei denen Texte wie Parteiprogramme oder Gesetzestexte gemeinsam von der Community erarbeitet und durch Abstimmungen beschlossen werden können.

Wir haben die von der Piratenpartei betriebene Plattform „Liquid Feedback“, die zwar öffentlich zugänglich ist, aber eine aktive Teilnahme nur Mitgliedern der Piratenpartei vorbehält, datenschutzrechtlich geprüft. Die Plattform ermöglicht jedem Mitglied, Parteitagsanträge einzureichen und Anträge anderer Mitglieder zu kommentieren. In einer zweiten Phase stimmen die Mitglieder über den jeweiligen Antrag sowie ggf. über Konkurrenzanträge ab. Jedes Mitglied kann seine Stimme für einzelne Abstimmungen oder auch für Themengebiete alternativ an ein anderes Mitglied delegieren, sodass sich Mitglieder auf bestimmte Themen spezialisieren können, aber dennoch alle Mitglieder – dann teilweise indirekt – über alle Themen und Anträge abstimmen können. Die Delegation einer Stimme kann zudem vor der Abstimmung jederzeit wieder entzogen werden, sodass die oder der Delegierte nur dann dauerhaft mit höherem Stimmgewicht zu bestimmten Themengebieten sprechen und abstimmen kann, wenn die Wünsche der vertretenen Mitglieder respektiert werden.

Da sämtliche Diskussionsprozesse und auch die Abstimmungsergebnisse transparent sind und internetöffentlich geführt werden, sind derartige Plattformen, die immer breiter in der Politik eingesetzt werden[56], sowohl aus Sicht der Informationsfreiheit als auch wegen der dabei auftretenden Datenschutzfragen interessant.

Die Teilnahme an innerparteilichen Willensbildungsprozessen ist bei den Piraten auch ohne die Nutzung der Plattform „Liquid Feedback“ sichergestellt, da

55 Vgl. http://liqd.net/

56 Bisher z.B. von der Enquete-Kommission des Deutschen Bundestages „Internet und digitale Gesellschaft“

die Abstimmungsergebnisse nur zur Unterstützung und Vorbereitung der Parteiarbeit eingesetzt werden. Verbindliche Abstimmungen über Anträge erfolgen auf Bundesebene konventionell auf einem halbjährlich stattfindenden Parteitag (vergleichbar auf Landesebene). In der Praxis hat sich jedoch gezeigt, dass in aller Regel die mittels „Liquid Feedback" vorbereiteten Anträge auf den Parteitagen ohne wesentliche Änderungen beschlossen werden.

Die Funktionalität der Plattform „Liquid Feedback" ist ein akzeptabler Kompromiss zwischen den Zielen der Transparenz und Überprüfbarkeit von Entscheidungsfindungen einerseits und des Datenschutzes andererseits. Die Mitglieder haben grundsätzlich die Möglichkeit, die Plattform unter **Pseudonym** zu nutzen. Auflösbar ist das Pseudonym nur unter bestimmten in der Satzung festgelegten Bedingungen. Dies wird technisch dadurch abgesichert, dass zur Aufdeckung eines Pseudonyms drei verschiedene Stellen oder Verantwortliche die entsprechenden Daten zusammenlegen müssen. Aus Gründen der Nachvollziehbarkeit kann ein Löschungsbegehren nicht individuell umgesetzt werden, d. h. einmal eingestellte Beiträge werden erst nach einer vorher festgelegten Zeitspanne gelöscht. An die Stelle der Löschung tritt die Anonymisierung: Jedes Mitglied kann jederzeit die Teilnahme am System beenden. Dabei wird der angezeigte Name (das Pseudonym) aus den jeweiligen Beiträgen entfernt. Zudem kann jedes Mitglied mit einem neuen Pseudonym, das nicht mit dem bisherigen Pseudonym verkettet werden kann, wieder am System teilnehmen.

Aus Datenschutzsicht nicht unproblematisch ist die Speicherdauer eines Antrages und des Abstimmungsverhaltens, da viele Mitglieder unter echtem Namen agieren. Aufgrund der Transparenz und der Überprüfbarkeit des Systems wird jedem Mitglied offenbart, wer (welches Pseudonym) wie über einen Antrag abgestimmt hat. Derzeit ist eine Speicherdauer von vier Parteitagen (ca. zwei Jahre) vorgesehen, damit ein neuer Vorstand Abstimmungsergebnisse prüfen kann. Für Parteimitglieder sind alle Informationen wie Anträge, Kommentare und nach einer Abstimmung die vom einzelnen Mitglied (dem Pseudonymen) abgegebene Stimme zugänglich. Die Piratenpartei begründet dies mit der Notwendigkeit, Transparenz und Überprüfbarkeit zu schaffen. Anderenfalls könnte dem System ähnlich wie bestimmten Wahlcomputern nicht vertraut werden.

Der Schutz der personenbezogenen Daten der aktiven Mitglieder[57] kann daher derzeit nur durch das Angebot eines pseudonymen Zugangs gewährleistet werden. Weiterentwicklungen zur Verbesserung der Privatsphäre wären dadurch denkbar, dass ein Mitglied z.B. unter mehreren verschiedenen Pseudonymen auftreten könnte. Dann müsste technisch sichergestellt werden, dass ein Mitglied z.B. nicht mehrfach abstimmen bzw. vielleicht auch nicht unter verschiedenen Pseudonymen gleichzeitig an einer Diskussion teilnehmen kann. Problematisch ist u.U., Stimmen an pseudonyme Mitglieder zu delegieren. Gegenüber der Öffentlichkeit wird Datenschutz dadurch gewährleistet, dass für Nichtmitglieder zwar alle Anträge, Diskussionen sowie die Abstimmungsergebnisse einsehbar sind, jedoch nur in anonymisierter Form: Alle Namen und Pseudonyme werden entfernt, und von Abstimmungen werden nur die **anonymisierten Ergebnisse** veröffentlicht.

Online-Plattformen zur Unterstützung basisdemokratischer Prozesse stehen im Spannungsverhältnis zwischen Informationsfreiheit und Datenschutz. Allerdings sind die Datenschutzprobleme durchaus lösbar. Die Plattform „Liquid Feedback" stellt eine aus Datenschutzsicht akzeptable, aber technisch noch weiterzuentwickelnde Lösung dar. An uns herangetragene Bedenken wurden teilweise durch Änderungen am System beseitigt, insbesondere die Begrenzung der Speicherdauer, die Möglichkeit, unter Pseudonym aufzutreten, sowie die Anonymisierung des öffentlich zugänglichen Webangebotes.

1.2.2 IT-Sicherheit

Weltweite Angriffe auf die Informationssicherheit

Lange Jahre war der Glaube weitverbreitet, dass sich jemand, der weder unbekannte E-Mail-Anhänge ausführt noch Hacker-, Crack- oder sonstige Schmuddelseiten besucht und seinen Rechner regelmäßig aktualisiert und mit Virenschutz und Firewall versieht, gegen bedrohliche Angriffe aus dem Internet geschützt fühlen kann. Doch neue Bedrohungen, welche von Viren, Trojanern,

57 Hierbei handelt es sich um sensitive personenbezogene Daten nach § 3 Abs. 9 BDSG.

Spionageprogrammen und anderem schadhaften Code ausgehen, sind oft nur noch einen Mausklick entfernt. Die Taktiken und die Beweggründe der Cyber-Kriminellen haben sich geändert. Es werden immer wieder Softwareschwachstellen aufgefunden und geschickt durch professionell arbeitende Hackergruppen ausgenutzt. Immer effektivere und lautlose Spionagemethoden bedrohen Regierungen, Wirtschaftsunternehmen und private Computer-Nutzer.

Im letzten Jahresbericht berichteten wir über die Abhängigkeit der Informationsgesellschaft von einer funktionierenden informationstechnischen Infrastruktur[58] und die kriegsähnlichen Bedrohungen, denen sie zum Teil ausgesetzt waren. In diesem Jahr füllten Schlagzeilen zu spektakulären Datendiebstählen und Angriffen auf Internetportale die Titelseiten der Weltpresse. Die folgende Aufzählung ist keineswegs abschließend:

- Hacker brachen mehrfach bei Sony ein, im April verschafften sie sich Zugang an die Daten von mehr als 100 Millionen Kunden, im Oktober an weitere 93.000 Nutzer-Konten.[59]
- Im Juni stahlen Cyber-Kriminelle 360.000 Datensätze der US-Bank City-Group.[60]
- Bei Rewe wurden im Juli 52.000 Kundendaten von Internet-Tauschbörsen für Tierbilder und Bilder der Frauen-Fußballweltmeisterschaft entwendet.[61]
- Im August erfolgte ein Einbruch beim Kryptospezialisten RSA[62], bei dem sicherheitsrelevante Daten zu einem Authentisierungssystem gestohlen wurden. In der Folge mussten 40 Millionen Hardware-Tokens ausgetauscht werden.
- Im August berichteten mehrere Zeitungen[63] über Spionageangriffe auf mindestens 72 Behörden, Organisationen und Unternehmen in 14 Ländern seit mindestens fünf Jahren.

58 Vgl. JB 2010, 1.1

59 „Neue Hacker-Attacke auf Sony", Magnus.de vom 12. Oktober 2011

60 „Cyber-Attacken: Wer ist das nächste Opfer?", Datenschutz-Berater Nr. 7+8 2011, S. 4

61 Ebenda

62 „RSA tauscht nach Hack bis zu 40 Millionen SecurID-Tokens aus", heise online vom 7. Juni 2011

63 „Hacker attackieren Regierungen, Firmen und die UN", Der Tagesspiegel vom 4. August 2011, S. 1; „Hacker führen Wirtschaftskrieg", Frankfurter Rundschau vom 4. August 2011, S. 12; „McAfee deckt Datendiebstahl im großen Stil auf", F.A.Z. vom 4. August 2011, S. 15

- In Südkorea wurden persönliche Daten von 35 Millionen Internetnutzern von zwei populären Online-Plattformen gestohlen.[64]
- Im September gab es 300 zielgerichtete und anhaltende Botnetz-Attacken gegen Rechenzentren und Firmen insbesondere in den GUS-Staaten, insgesamt wurden 1465 Computer in 61 Ländern infiziert[65].
- Das niederländische Unternehmen DigiNotar, das Zertifikate herausgab und Trustcenter für die Regierung betrieb, wurde Opfer eines Hacker-Angriffs und musste Insolvenz anmelden.[66]
- Im Oktober wurden in Schweden mittels SQL-Injection-Techniken über 210.000 Login-Daten von mindestens 60 Webservern erbeutet.[67]
- Der Sportartikelhersteller Adidas sperrte im November seine Internetseiten nach einem Hacker-Angriff.[68]
- Die Hackergruppe Anonymous griff im November israelische Webseiten an[69], Ziele waren u.a. die Armee, der Mossad und der Inlandsgeheimdienst Shin Beth.
- Die gleiche Gruppe erbeutete im Dezember bis zu 90.000 geheime Kundendaten mit Kreditkarteninformationen bei der amerikanischen Sicherheitsfirma Strategic Forecasting (Stratfor) und tätigte Geldtransfers im Wert von rd. einer Million Dollar an Wohlfahrtsorganisationen.[70]

Es stellt sich die Frage, ob die Sicherheit im Internet vollends außer Kontrolle gerät. Doch die Welle von Angriffen zeigt nun offensichtlich Wirkung. Der US-Marktforscher IDC hatte deutsche Firmen hierzu befragt. Ein Großteil der Befragten wird die Ausgaben für IT-Sicherheit aufstocken. Der Legendenbildung der angeblich nicht fassbaren Hacker-„Helden", die auch Trittbrettfahrer animieren, wirken erste Erfolge der Verfolger entgegen:

64 „Unternehmen schließen Lücken", Handelsblatt vom 8. August 2011, S. 24
65 „Erneut großangelegter Spionage-Hack entdeckt", Magnus.de vom 27. September 2011
66 „DigiNotar wird liquidiert", Heise-Meldung vom 21. September 2011
67 „Großer Datendiebstahl-Skandal in Schweden weitet sich aus", ITespresso.de vom 28. Oktober 2011
68 „Adidas sperrt Internetseiten nach Hacker-Angriff", Handelsblatt vom 7. November 2011, 25
69 „Anonymous greift israelische Webseiten an", taz vom 11. November 2011, S. 11; „Viele Fragen und ein Verdacht", Süddeutsche Zeitung vom 8. November 2011, S. 7
70 „Robin Hood mit Hacker-Maske", Süddeutsche Zeitung vom 27. Dezember 2011, S. 6; „Hacker gegen Hacker", Süddeutsche Zeitung vom 28. Dezember 2011, S. 19

- So berichtet der „Datenschutz-Berater“[71] über die Zerschlagung des Botnetzes[72] „Hulx/Kelihos“. Dieses Netz war für Spamversand, Diebstahl von Finanzdaten und von DDoS-Attacken bekannt. Hulx ist zwar noch nicht abgeschaltet, da noch nicht alle befallenen Clients bereinigt sind, aber die Cyber-Kriminellen haben die Kontrolle verloren.
- Weiterhin wurde in der gleichen Zeitschrift[73] über das Auffliegen eines griechischen Hackers und eines Hackerteams aus Spanien berichtet. Beide hatten verfolgbare Spuren hinterlassen.
- Dem FBI gelingt ein Schlag gegen internationale Internetbetrüger.[74] Hier wurde ein Cybercrime-Ring aus Estland ausgehoben, der mit sog. Klick-Betrug 14 Millionen Dollar erschlichen hatte.

Die meisten Angriffe nutzen Fehlverhalten der Nutzer oder nicht beseitigte Sicherheitslücken aus, gegen die meist Software-Korrekturen („Patches“-Flicken) helfen. Durch die Vielfalt an Bedrohungen ist die Arbeit zur Absicherung der IT-Infrastruktur zwar sehr aufwendig; aber wenn selbst sog. Sicherheitsfirmen ihre geheimen Daten unverschlüsselt auf ihren mit dem Internet verbundenen Servern speichern, werden wir noch viele Schlagzeilen der oben zitierten Art erhalten.

Neues zur IT-Sicherheitspolitik in Berlin

Die Berliner Verwaltung hat bisher noch keine vergleichbaren Schlagzeilen wegen Informationssicherheitsmängeln ertragen müssen. Dies darf sie aber nicht veranlassen, sich auf dem Erreichten auszuruhen.

Mit Rundschreiben vom 18. März 2011 hat der IT-Staatssekretär die Hauptverwaltung und die Bezirke darauf aufmerksam gemacht, dass auch die öffentliche Verwaltung des Landes Berlin auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik und auf die Sicherheit der verarbeiteten Informationen angewiesen ist. Es verweist dabei auf die auch im letzten Jahres-

71 Datenschutz-Berater Nr. 11, 2011, S. 7
72 JB 2009, 12.2
73 Datenschutz-Berater Nr. 7/8, 2011, S. 29
74 „FBI gelingt Schlag gegen internationale Internetbetrüger“, Handelsblatt vom 11. November 2011, S. 22

bericht dargestellten Themen „Google Street View“, „Wikileaks“ und „Stuxnet“, um damit deutlich zu machen, dass Informationssicherheit nicht mehr nur eine Expertendiskussion ist, sondern die ganze Gesellschaft betrifft und damit Sache der politisch Verantwortlichen ist. Der IT-Planungsrat hat die Informationssicherheit auf nationaler Ebene zu einem Schwerpunktthema gemacht. Auf Landesebene haben sich der Ausschuss für Verwaltungsreform, Kommunikations- und Informationstechnik sowie der Unterausschuss Datenschutz und Informationsfreiheit des Ausschusses für Inneres, Sicherheit und Ordnung wiederholt mit Fragen der Informationssicherheit in der Berliner Landesverwaltung befasst und auf notwendige Verbesserungen gedrängt.

Wir sehen uns durch diese Initiativen bei der Verfolgung eines seit Längerem verfolgten Anliegens bestärkt, dass es bei der Erstellung und Umsetzung der gesetzlich vorgeschriebenen Informationssicherheitskonzepte nicht bleiben kann. Zusätzlich muss ein IT-Sicherheitsmanagement eingerichtet werden, das dafür sorgt, dass ein einmal erreichtes Sicherheitsniveau erhalten bleibt und im Rahmen eines Informationssicherheitsprozesses eine stetige Überprüfung der Wirksamkeit angesichts der dynamischen Veränderung der IT-Infrastrukturen und dem Aufkommen neuer Sicherheitsrisiken erfolgt. Der Staatssekretär hat auch die aktive Unterstützung durch die Behördenleitungen eingefordert, ein Anliegen, dass nach unseren Beobachtungen überall noch selbstverständlicher werden muss. Er kündigte die Erstellung eines Musters für die behördlichen IT-Sicherheitsleitlinien an, die das IT-Sicherheitsmanagement der Behörden bestimmen sollen. Dieses Muster beruht auf einem Musterdokument des Bundesamtes für Sicherheit in der Informationstechnik (BSI).[75]

In eine Informationssicherheitsleitlinie gehört das Bekenntnis einer Behördenleitung zu dem Stellenwert der Informationssicherheit in ihrem Haus, zum Schutzbedarf hinsichtlich der Schutzziele, zum Wert der zu schützenden Informationen und zum Aufwand, der diesem Wert gerecht wird. Damit verbunden ist eine Abwägung der Risiken: Welche kann man hinnehmen und gegen welche müssen Maßnahmen ergriffen werden? Weiter sollten Vorgaben zu elementaren Sicherheitsmaßnahmen wie den Zutritts-, Zugangs- und Zugriffsschutz,

75 Das Berliner Musterdokument ist derzeit (2. Januar 2012) noch im Internet verfügbar. Das Musterdokument des BSI lässt sich unter https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/hilfmi/muster/musterrichtlinien/musterrichtlinien.html herunterladen.

zum Virenschutz, zur Internetsicherheit, zum Umgang mit Sicherheitsvorfällen und zur Notfallvorsorge gemacht werden. Die Verantwortlichkeiten sind ebenso festzulegen wie die personelle und finanzielle Ausstattung des Informationssicherheitsmanagements und die regelmäßige Erfolgskontrolle im Rahmen des Informationssicherheitsprozesses.

Soweit der von der politischen Führung des Landes angestrebte Soll-Zustand. Über den Ist-Zustand berichtet alljährlich der IT-Sicherheitsbericht, der seit dem Frühjahr für das Jahr 2010 vorliegt. Dabei muss man berücksichtigen, dass der Bericht auf den Auskünften der freiwillig teilnehmenden Behörden (in diesem Jahr 70) beruht, die zwar eine vorgegebene Struktur haben, deren Ausfüllung aber nicht auf gleichen Wertmaßstäben basiert. Die Anzahl der Behörden mit behördlichem Sicherheitskonzept ist deutlich gestiegen. Ein knappes Viertel der teilnehmenden Behörden hat aber immer noch keines, obwohl bereits seit 1999 Verwaltungsvorschriften Sicherheitskonzepte verlangen. Diese Behörden sind allerdings (mit einer Ausnahme) dabei, eines zu erstellen. Angaben zu den verfahrensspezifischen Sicherheitskonzepten, die seit 2001 gesetzlich vorgeschrieben sind, wurden nicht abgefragt. Von den vorliegenden Sicherheitskonzepten ist ein Drittel von den Behördenleitungen nicht bestätigt worden; die im Rundschreiben vom März eingeforderte aktive Unterstützung der Behördenleitungen ist also noch sehr lückenhaft. Nach wie vor gibt es Behörden (in diesem Jahr 11), die freimütig bekennen, dass sie für die Informationssicherheit keine Ressourcen zur Verfügung stellen. Das ist unverantwortlich.

Aus der Zusammenfassung des Berichts seien weitere Angaben hervorgehoben:

- Soweit Sicherheitskonzepte vorliegen, wurden sie in den allermeisten Fällen nach den Methoden der Grundschutz-Katalog des BSI oder des daraus abgeleiteten Modellsicherheitskonzepts entwickelt.
- In den meisten Behörden (43) werden nicht die erforderlichen Schulungen zur Informationssicherheit durchgeführt. Dies ist jedoch unabdingbarer Bestandteil zur Gewährleistung der Informationssicherheit.
- In fast allen (61) Behörden ist ein IT-Sicherheitsbeauftragter benannt, aber nur in der Hälfte von ihnen ist ein geregelter Informationssicherheitsprozess eingeleitet worden, der das vorhandene Sicherheitsniveau auf dem Stand halten kann.

- Die Wirksamkeit ihrer dezentralen Sicherheitsmaßnahmen wird von den Behörden als gut eingeschätzt, die Wirksamkeit der zentralen Sicherheitsmaßnahmen als sehr wirksam.
- Die gemeldeten Sicherheitsvorfälle beziehen sich fast alle auf Beeinträchtigungen oder den Verlust der Verfügbarkeit (Ausfall der Stromversorgung, Kabelschäden, Serverausfälle).
- Die größten Risiken sind Irrtümer und Nachlässigkeiten des eigenen Personals, Fehler und Qualitätsmängel der Hard- und Software und Schadsoftware.
- In 49 Behörden werden mobile Endgeräte wie Smartphones, Blackberrys und Tablet PCs (wie iPad) vereinzelt vor allem von Führungskräften verwendet, meist jedoch der Blackberry. Als wesentliches Risiko bei der Verwendung solcher Geräte wird der Verlust oder Diebstahl mit der Gefahr der Datenverlusts oder -missbrauchs gesehen. Es wird festgestellt, dass solche marktüblichen Geräte ohne umfangreiche Anpassungen nicht sicher im dienstlichen Umfeld betrieben werden können.

Weltweit werden die Unternehmen und Behörden mit immer heftigeren Angriffen auf ihre Informationssysteme und mit zunehmend gravierenden Folgen für die Betroffenen konfrontiert. Dagegen müssen sich die Berliner Behörden, aber auch die Berliner Unternehmen wappnen. Während diesbezügliche Kennzahlen für die Unternehmen nicht vorliegen, können wir für die Behörden konstatieren, dass die Informationssicherheit langsame, aber stetige Fortschritte macht. Noch immer sparen einige Behörden aber an der falschen Stelle, indem sie Verletzungen der Informationssicherheit in Kauf nehmen.

2. Schwerpunkte

2.1 Cloud Computing

2.1.1 Orientierungshilfe – Cloud Computing

Mehrere Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben eine „Orientierungshilfe – Cloud Computing“ erarbeitet, die von der Konferenz selbst und dem Düsseldorfer Kreis verabschiedet wurde.[76] Diese Orientierungshilfe enthält neben einer Analyse der technischen Risiken und datenschutzrechtlichen Fragen praktische Hinweise auf Möglichkeiten und Grenzen einer rechtskonformen Nutzung der verschiedenen Formen von Cloud-Angeboten. Zugleich wird die Orientierungshilfe Grundlage für die Prüftätigkeit der Datenschutzbehörden sein.

Cloud Computing ist Datenverarbeitung im Auftrag

Nimmt der Cloud-Anwender von einem Cloud-Anbieter IT-Dienstleistungen für Cloud-Services in Anspruch, so ist Letzterer Auftragnehmer im datenschutzrechtlichen Sinne. [77] Der Cloud-Anwender bleibt hingegen für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich. Weiterhin muss der Cloud-Anwender dem Cloud-Anbieter einen schriftlichen Auftrag erteilen und dabei die inhaltlichen Anforderungen der Datenschutzgesetze erfüllen.

Der Cloud-Anwender hat sich als Auftraggeber nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und danach regelmäßig von der Einhaltung der beim Cloud-Anbieter als Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Dem Cloud-Anwender wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen. Allerdings darf er sich nicht auf bloße Zusicherungen des Cloud-Anbieters

76 Vgl. Dokumentenband 2011, S. 22; die Orientierungshilfe selbst ist abrufbar unter http://www.lda.brandenburg.de/sixcms/media.php/2232/OH_Cloud_110926.pdf

77 § 11 Abs. 2 BDSG, § 3 Abs. 1 BlnDSG

verlassen, sondern er muss eigene Recherchen betreiben, um sich Gewissheit darüber zu verschaffen, dass gesetzlich normierte oder vertraglich vereinbarte Sicherheitsstandards eingehalten werden. Die Lösung kann darin bestehen, dass der Cloud-Anbieter sich einem Zertifizierungs- bzw. Gütesiegelverfahren zu Fragen des Datenschutzes und der Datensicherheit bei einer unabhängigen und kompetenten Prüfstelle unterwirft.

Fehlende Ortsgebundenheit der Datenverarbeitung und internationale Datentransfers

Public Clouds, die auf dem freien Markt angeboten und genutzt werden, sind nicht an geografische Grenzen gebunden, und die darin stattfindende Datenverarbeitung ist nicht ortsgebunden. Daher muss dem Anwender deutlich werden, wo die Cloud-Anbieter und deren Unter-Anbieter tätig sind. Der Cloud-Anwender wird aber oft nicht wissen, an welchem „Ort" im jeweiligen Augenblick die Verarbeitung erfolgt. Deshalb ist es wichtig, dass er sämtliche Verarbeitungsorte kennt und über jeden Wechsel des Verarbeitungsorts vorab informiert wird.

Erfolgen die Datenverarbeitungen außerhalb der EU und des EWR, indem die Cloud-Anbieter und/oder Unter-Anbieter eine Datenverarbeitung in Drittstaaten vornehmen, so gelten für den Transfer der Daten in Drittstaaten besondere gesetzliche Anforderungen.[78] Allerdings ist zu beachten, dass für die Anbieter in den Drittstaaten gegenüber ihren Regierungen gesetzliche Pflichten bestehen können, unter bestimmten Voraussetzungen transferierte Daten zu offenbaren (z.B. USA, Patriot Act). Ferner ist nicht ausgeschlossen, dass die Verarbeitung in Staaten stattfindet, in denen ein Schutz vor staatlichem Zugriff auf die Daten auch ohne gesetzliche Vorgaben nicht sichergestellt werden kann.

78 §§ 4b, 4c BDSG, § 14 BlnDSG

Cloud-spezifische Risiken

Eine wesentliche Eigenschaft des Cloud Computing ist, dass die Anwender Computerressourcen nutzen, auf die sie selbst keinen konkreten Zugriff haben. Daraus ergeben sich folgende Risiken:

- Das Löschen im Sinne des endgültigen Unkenntlichmachens von Daten kann nicht ohne Weiteres realisiert und überprüft werden.
- Die meisten Protokolle und Dokumentationen zur Datenverarbeitung in der Cloud befinden sich beim Cloud-Anbieter, sodass die darauf aufbauende Kontrolle nicht durch den verantwortlichen Cloud-Anwender, sondern nur durch den Cloud-Anbieter erfolgen kann.
- Anbieter von Cloud-Services sind gemeinhin an Standorten angesiedelt, die über extrem breitbandige Internet-Anbindungen verfügen. Diese leistungsfähigen Anbindungen sind notwendig. Sie ermöglichen es aber auch, in kürzester Zeit große Datenmengen an andere Standorte zu verschieben oder zu kopieren.

Neben diesen besonderen Risiken spielen auch in der Cloud die **klassischen Risiken** für die IT-Sicherheit eine wesentliche Rolle. So sind z.B. Angriffe mit Schadsoftware auf die Dienste in der Cloud denkbar. Auch kann die gebotene **Trennung der Daten** unterschiedlicher Anwender gefährdet sein.

Die T**ransparenz der Datenverarbeitung** in der Cloud ist für die aus der Ferne arbeitenden Cloud-Anwender ohne besondere Maßnahmen des Cloud-Anbieters kaum gegeben. Dies führt u.U. dazu, dass

- die Cloud-Anwender die Kontrolle über den Zugriff auf die eigenen Daten aufgeben,
- bei der Nutzung einer Public Cloud in Drittländern der Zugriff auf Daten des Cloud-Anwenders durch staatliche und private Stellen möglich und nicht kontrollierbar ist,
- Cloud-Anwender nicht über den Ort der Verarbeitung oder die Wege ihrer Daten durch die Cloud und die näheren Umstände der Verarbeitung beim Cloud-Anbieter informiert werden,

- Cloud-Anwender nicht kontrollieren können, ob die Umstände der Datenverarbeitung und die Maßnahmen zum organisatorischen Datenschutz beim Cloud-Anbieter den Verträgen zur Auftragsdatenverarbeitung gerecht werden,
- Cloud-Anwender keine Kontrolle über die Datenspuren haben, die sie bei der Nutzung der Cloud hinterlassen,
- Cloud-Anwender keine Kontrolle über Subunternehmer der Cloud-Anbieter haben, denen der Zugriff auf die Rechner ermöglicht wird.

Zusammenfassung

Die Anforderungen an die Datenverarbeitung der Unternehmen und Behörden, zu denen Datenschutz und Informationssicherheit, aber auch die Kontrollierbarkeit, Transparenz und Beeinflussbarkeit gehören, sind auch unter den Rahmenbedingungen des Cloud Computing, insbesondere in der Public Cloud, zu erfüllen. Es muss verhindert werden, dass die Fähigkeit der Organisationen, allen voran ihrer Leitungen, die Verantwortung für die eigene Datenverarbeitung noch tragen zu können, durch das Cloud Computing untergraben wird. Diese Verantwortung darf nicht „verdunsten".

Zu verlangen sind mindestens

- offene, transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Anwender klare Entscheidungskriterien bei der Wahl zwischen den Anbietern haben, aber auch, ob Cloud Computing überhaupt in Frage kommt,
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z.B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen" kann,
- die Umsetzung von abgestimmten Sicherheitsmaßnahmen auf Seiten von Cloud-Anbietern und Cloud-Anwendern,

- die Vorlage aktueller Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird, zur Gewährleistung der Informationssicherheit und der o. g. Portabilität und Interoperabilität durch anerkannte und unabhängige Prüfungsorganisationen.

Wir haben diese Mindestanforderungen an die Initiative **„Nationale Plattform Sichere Cloud“** im Rahmen der von der Bundesregierung unterstützten Forschungsunion Wirtschaft-Wissenschaft eingebracht. Dort soll ein Erprobungs- und Testumfeld für deutsche Sicherheitsanbieter entwickelt werden.

2.1.2 Cloud Computing in Berlin

Das ITDZ gab Ende 2010 den Startschuss zu einer „**Government-Cloud“**, um der Berliner Verwaltung künftig Cloud-Services anbieten zu können. Speicher- und Serverkapazitäten, Software und Rechenleistung können innerhalb des Berliner Landesnetzes in Anspruch genommen werden. Voraussetzung war die bereits seit mehreren Jahren erfolgte Virtualisierung des Serverparks des ITDZ.

Bei diesem Dienst handelt es sich um eine Private Cloud, bei der die typischen, in der Orientierungshilfe angesprochenen datenschutzrechtlichen Risiken nicht auftreten. Gleichwohl sind auch hier die rechtlichen Rahmenbedingungen der Auftragsdatenverarbeitung nach § 3 BlnDSG zu beachten und die vor allem mit dem Einsatz virtueller Maschinen zusammenhängenden Sicherheitsrisiken in den Sicherheitskonzepten zu berücksichtigen.

Ein bedeutendes Wirtschaftsunternehmen hat weniger sensitive, aber gleichwohl personenbezogene Datenverarbeitungen als „Infrastructure as a Service“ auf eine Public Cloud des amerikanischen Anbieters **Amazon World Service (AWS)** ausgelagert. AWS gibt seinen Kunden die Möglichkeit, bei der Registrierung und Parametrisierung des Dienstes den Verarbeitungsort selbst festzulegen, wobei sich das Wirtschaftsunternehmen für das irische Rechenzentrum des Anbieters entschied, um den rechtlichen Problemen des Transfers von personenbezogenen Daten in Drittstaaten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums zu entgehen. AWS garantierte, die Wünsche der europäischen Kunden strikt einzuhalten. Gleichwohl fand sich im Standardvertrag der Vorbehalt, dass ein Transfer der Daten in die USA

zu erfolgen hätte, wenn staatliche Stellen der USA dieses fordern würden. Das Wirtschaftsunternehmen ist unserer Forderung, andere Lösungen als die Beauftragung amerikanischer Unternehmen für die Datenverarbeitungen zu finden, bisher nicht gefolgt.

Google Text & Tabellen (Google Docs) ist ein Angebot von Google zur Erstellung und Speicherung von Dokumenten, Tabellen und Präsentationen, also zur Nutzung üblicher Office-Programme. Die Nutzung von Google Text & Tabellen unterscheidet sich jedoch in der normalen täglichen Anwendung von den übrigen Office-Paketen dadurch, dass die Verarbeitung über das Internet bei Google stattfindet und die erstellten Dateien bei Google gespeichert werden. Man kann auch Dateien beliebiger Dokumenten-Formate zu Google hochladen und dort verwalten. Bei dem Angebot von Google handelt es sich um ein Software-as-a-Service-Angebot in einer Public Cloud. Die Nutzung des Angebots führt zur Speicherung der Daten in einem Datencenter von Google, wobei der Ort der Speicherung nicht festgelegt ist, möglicherweise in den USA erfolgt. Damit greifen dann, wenn die Dokumente personenbezogene Daten erhalten, die verschärften rechtlichen Anforderungen bei Datentransfers in Drittstaaten und die Zugriffsvorbehalte der amerikanischen Administration.

Offenbar ist die Nutzung von Google Text & Tabellen auch zur Verwendung bei der Erstellung von Zeugnissen und dazugehörigen Listen in **Berliner Schulen** attraktiv. Eltern fragten uns, ob die Schule ihrer Kinder mit dem Einsatz von Google Docs rechtmäßig handelt. Der Schulleiter erklärte in seiner Stellungnahme, dass es nach seiner Meinung keine bessere Lösung der Textverarbeitungsaufgaben bei der Zeugniserstellung seiner Schule gäbe. Nach einem längeren Schriftwechsel mit dem Schulleiter teilte er mit, dass er die Nutzung von Google Docs eingestellt habe. Damit konnte von einer Beanstandung abgesehen werden.

Die Nutzung von Cloud-Diensten, bei denen personenbezogene Daten entweder in Länder ohne angemessenes Datenschutzniveau exportiert oder dem unkontrollierten Zugriff ausländischer Behörden ausgesetzt werden, ist unzulässig.

2.2 Aktuelle Datenschutzgesetzgebung in Berlin

2.2.1 Novellierung des Berliner Datenschutzgesetzes

Das seit Februar geltende Vierte Gesetz zur Änderung des Berliner Datenschutzgesetzes (BlnDSG)[79] hat zu verschiedenen Verbesserungen geführt. Die wichtigsten Änderungen werden im Folgenden dargestellt:

Der Landesgesetzgeber hat Konsequenzen aus dem Urteil des Europäischen Gerichtshofes (EuGH) vom 9. März 2010 gezogen und die Unabhängigkeit des Berliner Beauftragten für Datenschutz und Informationsfreiheit gestärkt.[80] Der EuGH hatte die Bundesrepublik Deutschland wegen der Verletzung von Gemeinschaftsrecht verurteilt, weil die Aufsicht über den Datenschutz in der Wirtschaft nicht – wie vorgeschrieben – in völliger Unabhängigkeit stattfand. In Umsetzung der Vorgaben des EuGH wurde die Rechtsaufsicht des Senats über den Berliner Beauftragten für Datenschutz und Informationsfreiheit gestrichen; der Dienstaufsicht des Präsidenten des Abgeordnetenhauses von Berlin unterliegt er nur insoweit, als seine Unabhängigkeit dadurch nicht beeinträchtigt wird.[81]

Die Mehrzahl der Änderungen des Berliner Datenschutzgesetzes erfolgte, um im Anschluss an die Novellierung des Bundesdatenschutzgesetzes (BDSG) in den Jahren 2009 und 2010 die bestehenden Verweisungen der aktuellen Rechtslage anzupassen und verschiedene Regelungen zur Stärkung des Datenschutzes zu übernehmen.

Nach der Novellierung müssen Behörden und öffentliche Stellen des Landes Berlin, die Dritte mit der Verarbeitung personenbezogener Daten beauftragen, den Umgang des Auftragnehmers mit den Daten entsprechend dem BDSG im Einzelnen festlegen. Die genaueren Festlegungen und Weisungen des Auftraggebers führen auch dazu, dass dieser die Einhaltung der Maßnahmen

79 Gesetz vom 2. Februar 2011, GVBl. S. 51
80 Vgl. JB 2010, Einleitung
81 § 22 Abs. 2 Satz 2 BlnDSG

besser überprüfen kann.[82] Wichtig ist der Hinweis, dass die neuen Mindestanforderungen für Auftragsdatenverarbeitungsverträge auch für Alt-Verträge gelten. Die Verwaltungen sind somit verpflichtet, alle Auftragsdatenverarbeitungsverträge zu überarbeiten.

§ 18 a BlnDSG verpflichtet entsprechend unserem Vorschlag öffentliche Stellen des Landes Berlin dazu, unverzüglich den Betroffenen und den Berliner Beauftragten für Datenschutz und Informationsfreiheit zu informieren, wenn personenbezogene Daten jemandem unrechtmäßig bekannt geworden sind und dies zu schwerwiegenden Beeinträchtigungen der schutzwürdigen Interessen der Betroffenen führen kann. § 18 a BlnDSG orientiert sich dabei an dem für die Wirtschaft geltenden § 42a BDSG, ist aber weitergehend, da § 42a BDSG nur für bestimmte Datenkategorien gilt.[83] Berlin hat damit als eines der ersten Bundesländer die Verpflichtung zur Information über Datenlecks auf die öffentliche Verwaltung erstreckt.

Durch die Novellierung wurde die Rechtsposition der oder des behördlichen Datenschutzbeauftragten gestärkt, indem das Arbeitsverhältnis unter einen besonderen Kündigungsschutz gestellt wird[84]. Auch hat der Berliner Gesetzgeber der bzw. dem behördlichen Datenschutzbeauftragten ein ausdrückliches Fort- und Weiterbildungsrecht eingeräumt.[85]

Die positiv zu beurteilenden Veränderungen des BlnDSG werden zu einer Verbesserung des Datenschutzes in Berlin beitragen.

2.2.2 Landeskrankenhausgesetz

Am 1. Oktober 2011 ist das neue Landeskrankenhausgesetz (LKG) in Kraft getreten.[86] Wir haben die Novellierung intensiv begleitet. Unsere Prüferfahrung hatte gezeigt, dass für eine Reihe von Abläufen in einem modernen Kran-

82 § 3 Abs. 1 Satz 4 BlnDSG
83 § 42a Satz 1 Nrn. 1 bis 4 BDSG; vgl. 11.2
84 § 19 a Abs. 2 Satz 4 und 5 BlnDSG
85 § 19 a Abs. 5 BlnDSG
86 GVBl. S. 483

kenhaus das alte Berliner Landeskrankenhausrecht unzureichende Regelungen enthielt.[87] Die Berliner Krankenhäuser haben in den vergangenen Jahren die Erbringung von nichtmedizinischen Leistungen zunehmend an Dritte übergeben oder in Tochterunternehmen ausgelagert. Viele Krankenhäuser kochen die Speisen für ihre Patientinnen und Patienten nicht mehr selbst und bedienen sich Externer, um Kranke von einem Standort zum anderen zu transportieren. Der Transporteur muss die Patientinnen und Patienten ansprechen können. Speziell zubereitete Speisen werden mit Namen versehen, um Verwechslungen auszuschließen.

Das novellierte Gesetz erlaubt die Bekanntgabe der Patientennamen an die Dienstleister dort, wo dies unumgänglich ist und die Nutzung von Daten eine untergeordnete Rolle spielt. Auch die Verarbeitung der Daten im Auftrag ist geregelt worden: Ein Krankenhaus kann die Rechenkapazitäten und technische Expertise eines anderen Krankenhauses nutzen. Auftragnehmern außerhalb eines Krankenhauses müssen die Daten so übergeben werden, dass es ihnen nicht möglich ist, einen Bezug zu den Patientinnen und Patienten herzustellen. Lässt ein Krankenhaus Teile seines Archivs durch Dritte aufbewahren, so müssen die Akten verschlossen bzw. verschlüsselt übergeben werden.

Häufig erbringen Dienstleister **Wartungsleistungen** an den im Krankenhaus benutzten Geräten und Systemen. Hierbei lässt sich nicht immer vermeiden, dass sie auch Patientendaten zu Gesicht bekommen. Das neue Krankenhausgesetz erlaubt eine solche Wartung, unterwirft sie jedoch strengen Anforderungen. Die Initiative zu jedem Wartungsvorgang muss vom Krankenhaus ausgehen, die Wartungsvorgänge unter seiner Kontrolle bleiben und von ihm protokolliert werden. Informationen über die Kranken dürfen nicht „abfließen". Die Dienstleister dürfen nur aus Deutschland oder einem anderen Land der EU heraus operieren.

Wenn eine Patientin oder ein Patient das Krankenhaus verlässt, schließt dieses die Patientenakte ab und gibt sie in das Archiv. Für elektronische Akten ist das Äquivalent die **Sperrung** der Akte: Nur noch für eng begrenzte Zwecke, etwa bei Nachfragen einer nachbehandelnden Ärztin oder eines nachbehandelnden

87 JB 2008,8.2.5

Arztes, darf auf die gesperrten bzw. archivierten Akten zugegriffen werden. Für die Sperrung gibt das neue Gesetz eine konkrete Frist vor.

Patientendaten werden nicht nur für die Behandlung und deren Abrechnung gegenüber den Versicherungen und Krankenkassen genutzt, sondern werden auch benötigt, um die Qualität der Behandlung zu erhöhen. Krankenhäuser und ihre spezialisierten Arbeitsgemeinschaften analysieren Daten aus der Versorgung hierzu zielgerichtet, um festzustellen, ob bestimmte Qualitätsparameter eingehalten werden. Schließlich sollen Daten aus der Behandlung auch für Forschungszwecke genutzt werden können.

Diesen Verarbeitungszwecken ist gemein, dass sie außerhalb der eigentlichen Behandlung stehen und es gar nicht oder nicht durchgängig erforderlich ist, dass die Verarbeitenden um die Identität der Patientinnen und Patienten wissen, mit deren Daten sie arbeiten. Daher verlangt der Gesetzgeber hier eine Vorgehen in drei Stufen: Zunächst soll das Krankenhaus prüfen, inwieweit sich die Ziele auch mit anonymen Daten erreichen lassen. So genügen oft anonyme Auszüge aus Patientenakten, um Studierende mit bestimmten Krankheitsbildern bekannt zu machen. Sollen über einen längeren Zeitraum Daten zu einer Patientin oder einem Patienten zusammengeführt werden, etwa für die **Qualitätssicherung** der Behandlung, so ist dies über ein Pseudonym möglich. Hierfür sind die klinischen Krebsregister[88] einiger Krankenhäuser ein gutes Beispiel. Nur wenn der angestrebte Zweck mit anonymisierten oder pseudonymisierten Daten nicht erreicht werden kann, darf der Patientenname offenbart werden.

Völlig neu regelt das novellierte Landeskrankenhausgesetz den Datenzugriff für **Forschungszwecke**. Die Patientinnen und Patienten sollen die Kontrolle darüber behalten, wie mit den Daten über ihre Erkrankung und die Behandlung geforscht wird. Sie sollen wissen, für welches Forschungsvorhaben die Daten eingesetzt und wem sie übermittelt werden. Nur in engen Grenzen kann Forschung ohne das Wissen und Wollen der Patientinnen und Patienten betrieben werden: Die Ärztinnen oder Ärzte, die eine Patientin oder einen Patienten behandelt haben, können für ihre eigene Forschung auf die Dokumentation der jeweiligen Behandlung zurückgreifen. Auch andere krankenhausinterne Forschung von hohem Allgemeininteresse darf auf die Behandlungsakten des

88 Siehe 7.2.4

Krankenhauses zurückgreifen. In jedem dieser Fälle müssen jedoch entgegenstehende Interessen der Patientin und des Patienten berücksichtigt werden, deren Geheimhaltungsinteresse mit dem Interesse am Forschungsresultat abgewogen wird.

An einrichtungsübergreifend Forschende, Forschungsregister und Probensammlungen darf ein Krankenhaus die Patientendaten nur ohne Patientennamen, allenfalls mit einem Pseudonym versehen, übermitteln. Veröffentlichungen der Forschungsergebnisse dürfen Patientennamen, andere identifizierende Merkmale oder Pseudonyme nur dann enthalten, wenn die Patientin oder der Patient ausdrücklich und im Wissen um die konkrete Veröffentlichung zugestimmt hat.

Das novellierte Landeskrankenhausgesetz mit seinen Regelungen zur Verarbeitung von Patientendaten ist ein wesentlicher Schritt zur Modernisierung des Datenschutzes in einem besonders wichtigen Bereich: Bei der Verarbeitung von Patientendaten. Die Verarbeitung dieser sensitiven Daten und die Grenzen zulässiger Offenbarung im erforderlichen Umfang wurden klar und in einem ausgewogenen Interessensausgleich geregelt. Die Berliner Krankenhäuser sind aufgefordert, die neuen Anforderungen insbesondere zur Verarbeitung von Patientendaten im Auftrag, zur Qualitätssicherung und zur Forschung unverzüglich umzusetzen.

2.2.3 Justizvollzugsdatenschutzgesetz

Bereits im Sommer 2009 informierte uns die Senatsverwaltung für Justiz darüber, dass die Erarbeitung eines Entwurfs für ein Justizvollzugsdatenschutzgesetz[89] geplant ist, um die bisher in verschiedenen Gesetzen festgeschriebenen Regelungen zur Zulässigkeit der Datenverarbeitung im Justizvollzug in einem Gesetz zu bündeln. Gleichzeitig wurden wir gebeten, eigene Vorschläge und Anregungen in dieses Gesetzgebungsvorhaben einzubringen. Dieser Bitte sind wir gern nachgekommen.

89 JVollzDSG

Ziel des Gesetzentwurfs war, das Datenschutzrecht im Bereich des Justizvollzuges grundlegend zu modernisieren und den aktuellen technischen sowie organisatorischen Möglichkeiten und Gegebenheiten anzupassen. Weiterhin war beabsichtigt, das informationelle Selbstbestimmungsrecht der Gefangenen zu stärken.

Im Entwurfsstadium des Gesetzes konnten wir einen verbesserten Schutz der Gefangenen im Bereich der Videoüberwachung in besonders gesicherten Hafträumen erreichen. Bislang gab es keine speziellen Regelungen zur Videoüberwachung eines solchen Haftraumes, in dem ein Gefangener für einen begrenzten Zeitraum untergebracht werden kann, wenn in erhöhtem Maße Fluchtgefahr oder die Gefahr von Eigen- oder Fremdverletzung besteht.[90] Es bestand hierdurch das Risiko, dass auch der Sanitärbereich, der in der Regel ohne Abgrenzung in besonders gesicherten Hafträumen integriert ist, per Videokamera überwacht wird. Nunmehr ist ausdrücklich geregelt, dass bei der Videoüberwachung besonders gesicherter Hafträume die Intimsphäre des gefangenen Menschen zu wahren ist.[91] Auf unsere Anregung hin ist nunmehr auch gesetzlich festgeschrieben, dass für ihn erkennbar sein muss, wann die Videokamera in Betrieb ist[92].

Weiterhin konnten wir erreichen, dass beim Auslesen elektronischer Datenspeicher wie etwa Mobilfunkgeräte, die Gefangene ohne Erlaubnis besitzen, die Beachtung des Schutzes des Kernbereichs der privaten Lebensgestaltung sowohl der Gefangenen selbst als auch Dritter gesetzlich vorgeschrieben ist.[93]

Positiv hervorzuheben sind die Neuregelungen zu den Einsichtsrechten der Gefangenen in ihre elektronisch geführten Gefangenenpersonalakten. Den Gefangenen wird im Gegensatz zur bisherigen Rechtslage[94] grundsätzlich die Möglichkeit eingeräumt, diese Akten ohne Angabe eines Grundes einzusehen.

90 § 88 Strafvollzugsgesetz (StVollzG)
91 § 21 Abs. 3 JVollzDSG
92 § 21 Abs. 2 Satz 4 JVollzDSG
93 § 25 Abs. 2 JVollzDSG
94 § 185 Satz 1 StVollzG

Zudem ist nunmehr gesetzlich klargestellt, dass das Informationsfreiheitsgesetz auch im Bereich des Justizvollzugs grundsätzlich Anwendung findet.[95] Zu dieser Frage wurde in der Vergangenheit von der Senatsverwaltung für Justiz die gegenteilige Auffassung vertreten.[96]

Allerdings wurde nicht allen unseren Empfehlungen entsprochen. Bei drei Regelungen ist dies besonders zu kritisieren:

Das Gesetz definiert ohne Not den Begriff der verantwortlichen Stelle in Abkehr von der bisherigen grundlegenden Systematik im Datenschutzrecht neu. Nach den jetzigen Vorschriften werden u.a. alle Justizvollzugsanstalten des Landes Berlin, das Krankenhaus des Justizvollzugs, die zentrale IT-Stelle, die Auskunftsstelle des Justizvollzugs und weitere (nicht abschließend aufgezählte) öffentliche Stellen im Geschäftsbereich der Senatsverwaltung für Justiz, die schwerpunktmäßig Aufgaben des Justizvollzugs wahrnehmen, als einheitliche Daten verarbeitende Stelle angesehen.[97] Demgegenüber geht das Berliner Datenschutzgesetz vom sog. funktionalen Behördenbegriff aus. Danach ist Daten verarbeitende Stelle jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt; nimmt diese unterschiedliche gesetzliche Aufgaben wahr, gilt diejenige Organisationseinheit als Daten verarbeitende Stelle, der die Aufgabe zugewiesen ist.[98]

Ebenso wird es zukünftig möglich sein, biometrische Merkmale des Gesichts, der Augen, der Hände, der Stimme und der Unterschrift der Gefangenen zu vollzuglichen Zwecken zu erheben und zu verarbeiten.[99] Dies soll insbesondere dazu dienen, Verwechslungen auszuschließen und die Befreiung von Gefangenen bei Besuchen zu vermeiden. Ein derart erheblicher Eingriff in die Persönlichkeitsrechte der Gefangenen ist für die genannten Zwecke nicht erforderlich. Der praktisch ohnehin kaum relevanten Gefahr einer Gefangenenverwechslung kann mit wesentlich milderen Mitteln, etwa einem Handgelenkband oder Anstaltskleidung während der Besuchszeit, vorgebeugt werden.

95 § 3 Satz 2 JVollzDSG
96 JB 2003, 4.9.3
97 § 4 Abs. 2 JVollzDSG
98 § 4 Abs. 3 Nr. 1 BlnDSG
99 § 17 JVollzDSG

Weiterhin ist es nunmehr gesetzlich erlaubt, zur Verhinderung einer Gefangenenbefreiung auch Besucherinnen und Besucher einer erkennungsdienstlichen Behandlung zu unterziehen, etwa in Form der Abnahme von Fingerabdrücken, der Aufnahme von Lichtbildern oder der Messung äußerlicher körperlicher Merkmale.[100] Auch dies ist nicht erforderlich, denn zur Erreichung des gewünschten Zwecks genügt es, die Gefangenen zu identifizieren.

Das Justizvollzugsdatenschutzgesetz ist insbesondere aufgrund seiner differenzierten Betrachtung und Bewertung der verschiedenen Formen von Datenerhebung, -verarbeitung und -nutzung im Justizvollzug ein wichtiger Schritt zu besserem Datenschutz. Es wird jedoch nicht in jeder Hinsicht dem selbst gestellten Ziel gerecht, ein modernes, fortschrittliches und alle Interessen berücksichtigendes Datenschutzgesetz für den Justizvollzug zu schaffen.

2.3 Soziale Netzwerke

Seit 2007 berichten wir regelmäßig über die Entwicklungen im Bereich sozialer Netzwerke. Die grundsätzlichen Probleme und einige noch immer gültige Tipps zum Umgang mit derartigen Netzwerken haben wir bereits 2008[101] und in einem Ratgeber[102] herausgearbeitet.

Hier sollen problematische neue Entwicklungen und Funktionen, insbesondere des Netzwerkes Facebook, aufgezeigt werden, da dieses Netzwerk mittlerweile auch bei Nutzenden aus Deutschland eine so marktdominierende Position erreicht hat, dass selbst Behörden glauben, entgegen dem Rat der Datenschutzbeauftragten und trotz vorhandener Gefahren sowie rechtlicher Unsicherheiten nicht auf eine Präsenz bei Facebook verzichten zu können. Folgende problematische Neuerungen sind sichtbar geworden:

100 § 24 i.V. m. § 17 Abs. 1 JVollzDSG
101 Vgl. JB 2008, 2.2
102 Siehe Fn. 107

Social Plugins

Waren soziale Netzwerke bisher in sich geschlossene Portale, die Nutzende aktiv besucht haben, haben mittlerweile sog. „Social Plugins“ wie der „Like-Button“ („Gefällt mir-Knopf“) von Facebook oder der „+1-Button“ von Google viele Angebote im offenen Internet erobert. Das Ziel ist, auf einfache Weise im Netzwerk verlinkte Freunde auf interessante Webangebote hinweisen zu können. Die Anbieter der Webangebote versprechen sich von der Einbindung sozialer Plugins eine Erhöhung der eigenen Reichweite, da jeder Klick auf den Button eine kostenlose und zugleich effektive Werbung für das eigene Angebot darstellt. Grundsätzlich gäbe es auch keine Einwände gegen derartige Buttons, wenn nur mit Einwilligung der Nutzenden – also nach dem Klick – eine Datenweitergabe an das soziale Netzwerk erfolgen würde. Tatsächlich werden aber zumeist bereits beim Aufruf einer Webseite, die ein „Social Plugin“ eingebunden hat, personenbezogene Daten an das jeweilige soziale Netzwerk übermittelt, bevor die Nutzerin oder der Nutzer das Plugin anklickt oder auch nur sieht. Ursache ist die Art der Einbindung des „Social Plugins“ als sog. iFrame: Beim Laden der eigentlichen Webseite (also z.B. „MeineZeitung.de“) wird der Browser angewiesen, eine weitere Webseite von dem sozialen Netzwerk zu laden und an der vorgesehenen Stelle innerhalb der anderen Webseite anzuzeigen. Über eine entsprechende Codierung in der aufgerufenen URL und zusätzlich durch die Übermittlung der kompletten Ursprungsadresse (des sog. Referrers) erfährt das soziale Netzwerk zumindest, welche IP-Adresse zu welchem Zeitpunkt die betreffende Webseite aufgerufen hat. Ist die oder der Nutzende zudem registriertes oder sogar eingeloggtes Mitglied des Netzwerkes, werden zudem Cookies übermittelt, die eine direkte Identifizierung, d. h. eine Verknüpfung mit dem jeweiligen Nutzerprofil ermöglichen. Faktisch kann das soziale Netzwerk auf diese Weise nicht nur alle Aktivitäten der Nutzenden auf der Plattform verfolgen, sondern auch einen Großteil aller externen Webseitenbesuche, wenn dort derartige Plugins eingebunden sind.

Nach dem deutschen Datenschutzrecht sind „Social Plugins“ nur in einer Ausgestaltung rechtskonform, die sicherstellt, dass erst dann eine Datenübermittlung an Dritte erfolgt, wenn die Nutzenden dies durch einen Klick bestätigt haben. Eine solche „Zwei-Klick-Lösung“ kann mit wenig Aufwand selbst erstellt oder aus dem Internet heruntergeladen werden. Die Ausgestaltung als iFrame ist dagegen rechtswidrig und kann aufsichtsbehördliche Maßnahmen nach sich ziehen. Darauf weisen wir verantwortliche Stellen im öffentlichen

und privaten Bereich regelmäßig hin. Bisher haben die meisten von uns angesprochenen Stellen (dazu zählten so unterschiedliche Anbieter wie politische Parteien und Medienunternehmen) ganz überwiegend die Einbindung der „Social Plugins“ rechtskonform umgestaltet.

Nutzende können unzulässige „Social Plugins“ in der Regel daran erkennen, dass neben oder unter dem Button eine Zahl der bisherigen Klicks auf den Button, Bilder anderer Nutzenden, die bereits geklickt haben, oder auch Inhalte einer korrespondierenden Seite innerhalb des Netzwerkes, wie z.B. ein Newsfeed, angezeigt werden. Da derzeit noch viele Webangebote derartige Plugins einsetzen, können wir Nutzenden nur empfehlen, diese zu blockieren. Für die meisten Browser existieren dafür Einstellungsmöglichkeiten oder es können Browser-Erweiterungen (z.B. Ghostery) installiert werden.

Profile von Organisationen

Auch Profile von Firmen, Organisationen oder gar Behörden in sozialen Netzwerken (bei Facebook: „Fanpages“) sind kritisch zu sehen. Das Hauptproblem ist, dass auf diese Weise Nutzende dazu animiert werden, die Seite einer Organisation bei dem oft amerikanischen Netzwerkbetreiber anstelle des gut kontrollierbaren Webangebots der jeweiligen Organisation in Deutschland zu besuchen. Schon beim Besuch einer solchen Seite erhält das soziale Netzwerk personenbezogene Daten über die eingeloggten Nutzenden: Für diese ist das anonyme Ansehen der Inhalte so praktisch unmöglich. Zusätzlich verlegen viele Organisationen Kontaktmöglichkeiten oder kommentierbare Newsticker auf solche Seiten – mit problematischen Folgen für den Datenschutz: Eine aktive Beteiligung (z.B. durch das Kommentieren einer Meldung) ist nur noch möglich, wenn man bereit ist, gegenüber jedem beliebigen Internetnutzer – nicht etwa nur gegenüber dem Anbieter der Seite – seine Identität offenzulegen. Deutsche Behörden und Firmen helfen so diesen Anbietern sozialer Netzwerke und auch beliebigen Dritten, die Internet-Nutzung personenbezogen auszuspähen.

Rechtlich ist der Betrieb einer „Fanpage“ bei Facebook vergleichbar mit dem Betrieb eines Webangebotes. Betreibt der Anbieter die Webseite nicht selbst, sondern lässt diese Dienstleistung durch einen Dritten erbringen, muss er mit diesem Dienstleister einen Vertrag zur Auftragsdatenverarbeitung schlie-

ßen, soweit dabei personenbezogene Daten der Nutzenden verarbeitet werden. Er bleibt zudem verantwortlich für die gesamte Datenverarbeitung. Ein solcher Vertrag kann mit Facebook derzeit nicht abgeschlossen werden, da Facebook weder bereit ist, seine Datenverarbeitungsprinzipien vollständig offenzulegen noch die Datenverarbeitung der Kontrolle des Fanpagebetreibers zu unterstellen. Des Weiteren führt Facebook auf den „Fanpages" eine sog. **Reichweitenanalyse** durch, d. h. das soziale Netzwerk erstellt mit den Besucherdaten Statistiken über die Nutzung der „Fanpage". Dies wäre nur zulässig, wenn bei personenbezogenen Daten eine Einwilligung der Nutzenden eingeholt bzw. bei einer pseudonymisierten Verarbeitung zumindest ein Widerspruchsrecht eingeräumt werden würde.[103] Beides ist nicht vorgesehen: Eine Widerspruchsmöglichkeit existiert nicht, und die Dokumente, die Facebook-Nutzende bei Anmeldung zur Kenntnis nehmen müssen, erfüllen bisher nicht die Anforderungen an eine datenschutzrechtliche Einwilligung nach dem Bundesdatenschutzgesetz.

Zusammenfassend ist festzustellen, dass die bisherige Ausgestaltung der „Fanpages" durch Facebook einen datenschutzkonformen Betrieb nicht gestattet. Solange sich das Unternehmen weigert, die entsprechenden Voraussetzungen in seinem Angebot zu schaffen[104], ist von einer Nutzung von „Fanpages" bei Facebook nachdrücklich abzuraten. Öffentliche Stellen oder Unternehmen in Berlin, die an der beschriebenen datenschutzwidrigen Praxis festhalten, müssen mit Beanstandungen und aufsichtsbehördlichen Maßnahmen rechnen.

Wir haben im Rahmen der Koordinationsgespräche bei der Senatsverwaltung für Inneres und auch gegenüber der Senatskanzlei auf deren Nachfrage auf die Problematik hingewiesen und von einer Nutzung der betreffenden Angebote nachdrücklich abgeraten. Dem Senat haben wir darüber hinaus empfohlen, auch selbst bei der Facebook Inc. auf entsprechende Änderungen in Bezug auf „Fanpages" und „Social Plugins" durch das Unternehmen zu dringen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis") haben nochmals auf die Verpflichtung zur Einhaltung

103 § 15 Abs. 3 TMG

104 Z. B. eine Möglichkeit zum Verzicht auf die Facebook-Reichweitenmessung für den Inhaber der „Fanpage" und eine dementsprechende Reduktion der Verarbeitung von Nutzungsdaten durch Facebook im Widerspruchsfall

des geltenden Datenschutzrechts u.a. bei der Einbindung von „Social Plugins“ und dem Betrieb von „Fanpages“ hingewiesen.[105] Sie haben ihre Erwartung ausgedrückt, dass Anbieter sozialer Netzwerke sich an den hiesigen Datenschutzstandards auch dann orientieren, wenn sie ihren Unternehmenssitz außerhalb Deutschlands oder sogar des Europäischen Wirtschaftsraums haben.

Gesichtserkennung

Facebook und andere Onlinedienste bieten die Möglichkeit, Personen auf hochgeladenen Fotos zu erkennen und ggf. (halb-)automatisch mit dem Profil der Person zu verlinken. Aus Sicht der Privatsphäre problematisch ist an dieser Funktion, dass sie die Erhebung, Speicherung und Nutzung biometrischer Daten dieser Personen voraussetzt. Für ein soziales Netzwerk von der Größe von Facebook bedeutet dies, dass – bisher ohne Einwilligung und ohne Information der Betroffenen – biometrische Daten von 800 Millionen Menschen erhoben wurden. Diese Daten könnten auch verwendet werden, um Menschen auf den Aufzeichnungen von Überwachungskameras oder auch Smartphone-Kameras zu identifizieren – eine Horrorvorstellung, die derzeit nur noch dadurch behindert wird, dass die Rate der falschen Treffer zu hoch ist. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat aus diesem Grund ein Verwaltungsverfahren gegen Facebook eingeleitet. Dagegen holt die Google Inc. in ihrem Konkurrenzprodukt „FindMyFace“, das im Rahmen des sozialen Netzwerks Google+ angeboten wird, wie vorgeschrieben eine Einwilligung der Betroffenen ein. Daraus muss man folgern, dass dieser rechtskonformen Ausgestaltung auch betriebswirtschaftliche Überlegungen nicht entgegenstehen müssen. Umso unverständlicher ist es, dass Facebook sich weiterhin weigert, die entsprechenden datenschutzrechtlichen Bestimmungen einzuhalten.

Timeline

Eine populäre Funktion sozialer Netzwerke ist ein Datenstrom von Neuigkeiten über die Profilinhaberin bzw. den Profilinhaber. Dieser sog. Newsfeed soll bei Facebook (Timeline/Chronik) künftig einerseits mittels Smartphone-Apps

105 Beschluss vom 8. Dezember 2011: Datenschutz in sozialen Netzwerken, Dokumentenband 2011, S. 35

und Webangeboten Dritter auch automatisch „gefüttert“ werden und andererseits nicht mehr nur die letzten Aktivitäten enthalten, sondern zu einem lebenslangen Protokoll (Logfile) werden, welches in der Standardeinstellung für alle Profilbesucher zugänglich ist.

Profilinhabern kann nur geraten werden, diese Funktion grundsätzlich zu deaktivieren oder zumindest in Bezug auf ihre Reichweite in die Vergangenheit zu beschränken. Zudem sollte man keiner App und keiner Webseite gestatten, Daten ungefragt in den Newsfeed zu schreiben. Die Betreiber von sozialen Netzwerken sind aufgefordert, derartige Funktionen grundsätzlich erst nach expliziter Einwilligung zu aktivieren.[106]

Unabhängig davon empfehlen wir weiterhin, mit der Veröffentlichung eigener personenbezogener Daten in sozialen Netzwerken sparsam zu sein und sich dort unter Pseudonym zu bewegen.[107]

Fortentwicklung des Datenschutzrechts für soziale Netzwerke

Im März hat Hessen den Entwurf eines Gesetzes zur Änderung des Telemediengesetzes in den Bundesrat eingebracht. Damit sollte für die Nutzenden von Internetangeboten mehr Transparenz bei der Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten geschaffen werden. Dies sollte durch die Einführung von Verpflichtungen der Diensteanbieter zur Information der Nutzenden über Datenverarbeitungsprozesse und die gesetzliche Festlegung weiterer Maßnahmen geschehen, die auch für in der Internetnutzung weniger versierte Nutzende ein Mindestmaß an Datensicherheit gewährleisten sollen.

Wir haben der zuständigen Senatsverwaltung für Wirtschaft, Technologie und Frauen empfohlen, dass Berlin diesen Gesetzentwurf als wichtigen Teilschritt zur Verbesserung des Schutzes personenbezogener Daten im Internet und insbesondere in sozialen Netzwerken unterstützt. Nachdem der Bundesrat

106 Nach Ende des Berichtszeitraums kündigte Facebook an, es werde bei allen Nutzern das Profil durch die Timeline ersetzen. Dem kann man nur durch vollständige Abmeldung vom Netzwerk entgehen.

107 Vgl. die Broschüre „Ich suche Dich. Wer bist Du?“, die wir gemeinsam mit jugendnetz-berlin.de herausgegeben haben und die in unserem Internet-Angebot heruntergeladen werden kann.

den Gesetzentwurf einstimmig angenommen hatte, wurde er im Bundestag gestoppt. In ihrer Stellungnahme[108] äußerte sich die Bundesregierung überwiegend ablehnend zu dem Gesetzesentwurf und spricht sich für eine europäische Regelung anstatt nationaler Rechtsvorschriften aus sowie für Maßnahmen zur Selbstregulierung z.B. durch Verhaltenskodizes.

Damit hat die Bundesregierung unverständlicherweise ihrer Ankündigung vom letzten Jahr, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Hinweis darauf, dass Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem aktuellen Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzern nicht gerecht. Der Hinweis auf die Notwendigkeit gesetzgeberischen Handelns auf europäischer Ebene ist zwar richtig, verkennt aber, dass in der europäischen Debatte natürlich auf die in den Mitgliedstaaten vorhandenen Rechtsvorschriften zurückgegriffen wird und insoweit eine vorherige Änderung des Telemediengesetzes in der oben beschriebenen Form auch die Debatte auf europäischer Ebene entscheidend voranbringen könnte. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat den Gesetzentwurf des Bundesrates als einen Schritt in die richtige Richtung begrüßt.[109]

Verhaltenskodex für soziale Netzwerke

Zu möglichen Selbstverpflichtungen der Anbieter von sozialen Netzwerken hat am 2. November im Bundesministerium des Innern ein Gespräch stattgefunden, an dem der Berliner Beauftragte für Datenschutz und Informationsfreiheit gemeinsam mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Vorsitzender des Düsseldorfer Kreises) teilgenommen hat. Bei diesem Gespräch haben wir betont, dass der Datenschutz in sozialen Netzwerken dringend verbessert werden muss.[110] Dazu könnten auch Selbstverpflichtungen unter bestimmten Bedingungen beitragen:

108 BT-Drs. 17/6765 vom 3. August 2011

109 Entschließung vom 28./29. September 2011: Datenschutz bei sozialen Netzwerken jetzt verwirklichen!, Dokumentenband 2011, S. 18

110 Vgl. dazu die Gemeinsame Presseerklärung der Landesbeauftragten für Datenschutz und Informationsfreiheit in Berlin und Nordrhein-Westfalen vom 3. November 2011: Verhaltenskodex für soziale Netzwerke nur mit den Aufsichtsbehörden

- Freiwillige Selbstverpflichtungen oder Verhaltensregeln müssen die Einhaltung und Umsetzung des geltenden Datenschutzrechts fördern, können sie aber nicht ersetzen. Es reicht nicht, wenn sie lediglich das datenschutzrechtliche Minimum beschreiben.
- Verhaltensregeln müssen wirksame Sanktionsmöglichkeiten enthalten.
- Anbieter sozialer Netzwerke müssen für größtmögliche Transparenz sorgen, damit die Nutzenden die Kontrolle über ihre Daten zurückerhalten.
- Entsprechend den gesetzlichen Bestimmungen muss ein Verhaltenskodex zumindest das Verbot der Profilbildung konkretisieren, das Recht auf anonyme oder pseudonyme Nutzung der Netzwerke unterstreichen und sicherstellen, dass sämtliche Nutzungsdaten auf Wunsch der Nutzenden, jedenfalls nach Ende der Mitgliedschaft gelöscht werden.
- Die Voreinstellungen müssen – anders als bisher in den Netzwerken üblich – einen größtmöglichen Schutz der Privatsphäre erlauben.
- Die Netzwerkmitglieder müssen einfache Werkzeuge zur Durchsetzung ihrer Rechte auf Auskunft, Berichtigung und Löschung erhalten; sie sollten ihr Profil auch unkompliziert beim Wechsel zu anderen Netzwerken „umziehen“ können.
- Die technische Sicherheit in den Netzwerken muss nachweislich gewährleistet werden.
- Schließlich sind besondere Vorkehrungen zum Schutz von Minderjährigen zu treffen, deren Daten in sozialen Netzwerken besonders schutzwürdig sind.

Nur freiwillige Selbstverpflichtungen, die diese Voraussetzungen erfüllen und auch umgesetzt werden, könnten den Datenschutz in den sozialen Netzwerken stärken. Verhaltensregeln tragen nur dann zur Rechtssicherheit bei, wenn sie den Aufsichtsbehörden nach dem Bundesdatenschutzgesetz zur Prüfung vorgelegt werden. Im Falle der Freiwilligen Selbstkontrolle Multimedia, die vom Bundesministerium des Innern mit der Durchführung dieser Initiative beauftragt ist, wäre dies der Berliner Beauftragte für Datenschutz und Informationsfreiheit.

„Social Plugins“ oder „Fanpages“ von sozialen Netzwerken, die ohne Rechtsgrundlage personenbezogene Daten in die USA übermitteln, sind rechtswidrig und dürfen deshalb von Berliner Behörden oder Unternehmen nicht genutzt werden.

2.4 Videoüberwachung der Intimsphäre

Im vergangenen Jahr ist der Einsatz von Videoüberwachungsanlagen durch Unternehmen und andere private Datenverarbeiter weiter stark angestiegen. Das belegt die Vielzahl der Beschwerden von betroffenen Menschen, die uns erreicht hat. Auffällig ist dabei, dass immer häufiger Videokameras in öffentlich zugänglichen Bereichen installiert wurden, die als sensitiv einzustufen sind. Als sensitiv werden Bereiche bezeichnet, in denen Personen ihre religiösen oder philosophischen Überzeugungen, ihre politische Gesinnung oder ihre Sexualität frei entfalten können. Zu sensitiven Bereichen gehören z.B. Eingangsbereiche zu Kirchen, Partei- und Gewerkschaftsräumen, Nachtclubs und Bordellen, HIV-/ AIDS-, Suchtberatungsstellen oder Treffpunkte von Homosexuellen. Darüber hinaus gelten auch Umkleidekabinen in Kaufhäusern, Frei- und Hallenbädern als sensitiv, wenn sich Personen in diesen Bereichen entkleiden und die Videoüberwachung damit in den Kernbereich der Intimsphäre eingreift.[111] Gleiches trifft auf Behandlungszimmer von Arztpraxen oder sonstigen medizinischen Einrichtungen zumindest dann zu, wenn die Videoaufnahmen Rückschlüsse auf die Krankheit einer bestimmten Person zulassen.[112] Sensitive Daten unterliegen einem erhöhten gesetzlichen Schutz.[113]

Bei Freizeit- und Erholungseinrichtungen handelt es sich dann um sensitive Bereiche, wenn sie über Dusch-, Umkleide- und Wellness-Bereiche verfügen. Die Interessen der Besucherinnen und Besucher solcher Einrichtungen wie Saunen, Thermen, Dampfbäder, Massagestudios, Frei- und Hallenbäder sind besonders zu schützen. Die Eingriffsintensität in die Privat- und Intimsphäre dieser Personen ist aufgrund der Tatsache, dass es sich in vielen Bereichen innerhalb dieser Einrichtungen überwiegend um textilfreie Bereiche handelt, erheblich. Besonders schwerwiegend ist eine Videoüberwachung in diesen Bereiche dann, wenn nicht nur Erwachsene, sondern auch Kinder und Jugendliche in das Beobachtungsfeld der Kameras geraten.

Aus diesem Grund sollten verantwortliche Stellen statt des Einsatzes von Videokameras zuvor mildere Mittel prüfen, die geeignet sind, ihre Zwecke gleichermaßen zu erfüllen. Dabei sollten sie darauf achten, dass die schutzwürdigen

111 Vgl. JB 2008, 3.1.4
112 Vgl. JB 2002, 3.1
113 § 3 Abs. 9 BDSG

Interessen ihrer Besucherinnen und Besucher auch durch alternative Maßnahmen nicht verletzt werden. Wenn z.B. im Umkleidebereich eines Hallenbades regelmäßig Spindschrankaufbrüche und Diebstähle von Wertgegenständen festgestellt werden, sollte der Betreiber über die Verbesserung eines Schließsystems an den Spinden oder über die Verstärkung der Spindtüren nachdenken. Eine andere Alternative wäre die Errichtung von separaten Schließfachschränken außerhalb des Umkleidebereichs. Diese Maßnahme ermöglicht, Wertgegenstände sicherer zu verschließen als in Spindschränken. Die Videoüberwachung von Schließfachschränken außerhalb des sensitiven Umkleidebereichs wäre datenschutzrechtlich nicht zu beanstanden. Zusätzlich zu diesen Sicherungsmaßnahmen sollte der Einsatz von Personal verstärkt werden, das regelmäßige Kontrollrundgänge im Umkleidebereich durchführt. Manchmal kann eine unzulässige Erhebung sensitiver Daten durch eine Veränderung des Blickwinkels oder der Position der Kamera vermieden werden. So kann eine Kamera derart gedreht oder abgedeckt werden, dass nur der Eingang zu einem Umkleidebereich, nicht aber der Umkleidebereich selbst überwacht wird.

Einige verantwortliche Stellen geben als Grund für die Installation von Videokameras in ihren Einrichtungen die steigende Anzahl von Diebstählen an. Durch die erhebliche Eingriffsintensität in die Privat- und Intimsphäre der Besucherinnen und Besucher sind jedoch die schutzwürdigen Interessen der Betroffenen höher zu gewichten als die berechtigten Interessen der verantwortlichen Stelle. Im Ergebnis ist festzustellen, dass die Erhebung und Speicherung sensitiver Bilddaten in Umkleidebereichen nicht zulässig ist.

Ein anderes Beispiel für sensitive Bereiche sind Krankenhäuser. Hier muss zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Bereichen differenziert werden. Haupteingangsbereiche von Krankenhäusern können im Allgemeinen von Patientinnen und Patienten, deren Angehörigen und Gästen ebenso wie von Pflegepersonal und Servicekräften uneingeschränkt betreten werden. Das gleiche gilt für Anmeldebereiche und Wartezimmer in Arztpraxen. Diese Bereiche gelten in der Regel als öffentlich zugänglich.

Innerhalb von Krankenhäusern ist allerdings ein besonderer Aspekt zu beachten. Hier kann es leicht dazu kommen, dass durch die Videoüberwachung sensitive Gesundheitsdaten erfasst werden, die zum Kernbereich des Persönlichkeitsrechts gehören. Die Aufzeichnungen solcher Daten kann nicht mit einem

Hinweis auf das Hausrecht oder jedem sonstigen Interesse gerechtfertigt werden. Ähnlich problematisch ist die Videoüberwachung in Patientenzimmern. Sie gelten in der Regel nicht als öffentlich zugängliche Bereiche, sodass § 6b BDSG nicht angewendet werden kann. Die Videoüberwachung in Patientenzimmern ist nur ausnahmsweise und unter bestimmten Voraussetzungen zulässig, z.B. wenn dies aus medizinischen Gründen erforderlich ist.

Die Entscheidung, ob eine Videoüberwachung in sensitiven Bereichen zulässig ist, kann nur im Einzelfall getroffen werden. Die für die Videoüberwachungsmaßnahme verantwortliche Stelle hat – ggf. mit ihrem betrieblichen Datenschutzbeauftragten – vorab zu prüfen, ob eine Kamerainstallation zulässig sein kann. Nach § 6b Abs. 1 Nr. 3 BDSG ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Für die Bewertung der Videoüberwachung in anderen sensitiven Bereichen reicht die Videoüberwachungsvorschrift des § 6b BDSG indes nicht aus. Betrachtet man z.B. bestimmte Bereiche innerhalb von Krankenhäusern, Seniorenheimen oder speziellen Pflegeeinrichtungen, müssen andere Rechtsnormen herangezogen werden. Für den Justizvollzug ist gerade eine entsprechende Regelung getroffen worden.[114] Mit § 28 BDSG steht eine Regelung zur Verarbeitung sensitiver Daten zur Verfügung, die sich nicht – wie § 6b BDSG – auf die Datenerhebung mit optisch-elektronischen Einrichtungen beschränkt. Die in § 28 Abs. 6 - 9 BDSG formulierten Vorschriften sind darüber hinaus auch auf Videobeobachtungen im nicht öffentlich zugänglichen Raum anwendbar. Doch ganz gleich, ob § 6b BDSG oder § 28 BDSG beim Einsatz von Videoüberwachung in sensitiven Bereichen Anwendung findet, die in beiden Vorschriften formulierten Anforderungen können von den verantwortlichen Stellen nur selten erfüllt werden.

In der Regel ist die Videoüberwachung in sensitiven Bereichen unzulässig. In Ausnahmefällen muss ihre datenschutzrechtliche Zulässigkeit nach §§ 6b und 28 BDSG geprüft werden.

114 Vgl. 2.2.3

3. Öffentliche Sicherheit

3.1 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Bereits 2006 fanden anlässlich der Fußball-Weltmeisterschaft umfangreiche Zuverlässigkeitsüberprüfungen von Beteiligten statt.[115] Auch im Zusammenhang mit der Leichtathletik-Weltmeisterschaft 2009 wurden Personen überprüft, die zu bestimmten sicherheitsrelevanten Bereichen Zugang erhalten wollten.[116] In beiden Fällen wurde die Rechtmäßigkeit der Datenverarbeitung durch die Polizei auf Einwilligungserklärungen der Betroffenen gestützt.

Die Zulässigkeit einer Datenverarbeitung kann sich zwar grundsätzlich aus einer Einwilligung oder einer gesetzlichen Befugnis ergeben. Jedoch darf die Polizei auch beim Vorliegen entsprechender Einwilligungen nur solche personenbezogenen Daten verarbeiten, die sie für ihre Aufgabenerfüllung benötigt.[117] Die allgemeine Zuverlässigkeitsüberprüfung im Interesse von Großveranstaltern gehörte bislang nicht zu den Aufgaben der Polizei. Wir haben daher auf klarstellenden gesetzlichen Regelungen für Zuverlässigkeitsüberprüfungen bestanden. Das Abgeordnetenhaus hat sich dieser Auffassung angeschlossen und den Senat 2009 dazu aufgefordert, bei der nächsten Senatsvorlage zur Änderung des ASOG eine solche Regelung vorzusehen.[118]

Mit Wirkung vom 27. Juli 2011 ist eine entsprechende Regelung in das ASOG eingefügt worden.[119] Danach darf die Polizei, soweit eine Zuverlässigkeitsüberprüfung wegen besonderer Gefahren bei Großveranstaltungen erforderlich ist, personenbezogene Daten an öffentliche und nicht öffentliche Stellen übermitteln, wenn die Betroffenen schriftlich eingewilligt haben und die Übermittlung im Hinblick auf den Anlass der Überprüfung, insbesondere den Zugang der Betroffenen zu der Veranstaltung aufgrund eines berechtigten Sicherheits-

115 JB 2006, 2.2
116 JB 2009, 3.3
117 Vgl. JB 2007, 3.1.7
118 Vgl. JB 2009, Anhang 1
119 § 45a ASOG

interesses des Empfängers sowie wegen der Art und des Umfanges der Erkenntnisse über den Betroffenen angemessen ist. Dem Veranstalter darf nur mitgeteilt werden, dass Sicherheitsbedenken bestehen, nicht etwa, welche das sind. Die Betroffenen sind über den konkreten Inhalt der Übermittlung und die Empfänger ihrer personenbezogenen Daten aufzuklären. Die übermittelten Daten dürfen nur zweckgebunden verarbeitet werden, worüber der jeweilige Empfänger von der Polizei schriftlich zu unterrichten ist. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist zu unterrichten, wenn eine Datenübermittlung zum Zweck der Zuverlässigkeitsüberprüfung bei Großveranstaltungen beabsichtigt ist.[120]

Wir hatten uns im Vorfeld der Gesetzesänderung dafür ausgesprochen, Journalisten von derartigen Zuverlässigkeitsüberprüfungen auszunehmen. Das Abgeordnetenhaus ist dem nicht gefolgt, sondern hat auf Vorschlag des Senats eine Regelung beschlossen, die in der Praxis auf Schwierigkeiten stößt.

Eine Datenübermittlung bei Journalisten ist nur zulässig, wenn diese innerhalb der letzten zwölf Monate nicht bereits von einer anderen Polizeibehörde des Bundes oder eines Landes zuverlässigkeitsüberprüft wurden.[121] Diese Norm lässt sich allerdings nur umsetzen, wenn die anderen Polizeibehörden das Ergebnis ihrer Überprüfung nicht vor Ablauf von zwölf Monaten löschen. Eine frühzeitige Löschung ist aber aus Gründen des Datenschutzes geboten und wird auch praktiziert (z.B. in Bayern nach drei Monaten). Journalisten, die von anderen Polizeibehörden überprüft worden sind, müssen sich im selben Jahr in Berlin nur dann nicht erneut überprüfen lassen, wenn sie eine Bescheinigung über das Ergebnis der auswärtigen Überprüfung innerhalb des letzten Jahres vorweisen können.

Mit der Verabschiedung einer gesetzlichen Vorschrift zur Zulässigkeit von polizeilichen Zuverlässigkeitsüberprüfungen bei gefährdeten Großveranstaltungen hat der Gesetzgeber Rechtssicherheit geschaffen.

120 § 45a Abs. 3 ASOG
121 § 45a Abs. 1 Satz 4 ASOG

3.2 Videoüberwachung in der Liebigstraße

Im Sommer hatte die Polizei den Dachbereich eines geräumten Hauses in der Liebigstraße verdeckt von einer benachbarten Grundschule aus videoüberwacht. Der Polizeipräsident begründete diese Maßnahme mit der Verfolgung von festgestellten Straftaten von erheblicher Bedeutung sowie der Verhinderung weiterer Straftaten aus dem linksextremistischen Umfeld. Die Maßnahme erfolgte aufgrund einer polizeilichen Anordnung.[122] Die Anordnung enthält keine konkreten Einzelheiten zu Art und Weise der Durchführung der ideoüberwachung und nennt als weiteres Ziel der Maßnahme die Identifizierung derzeit unbekannter Personen der linksextremistischen Szene. Eine richterliche Anordnung wurde nicht beantragt.

Die Durchführung der Maßnahme in dieser Form war unzulässig. Die Polizei kann personenbezogene Daten durch einen verdeckten Einsatz technischer Mittel, insbesondere zur Anfertigung von Bildaufnahmen oder -aufzeichnungen erheben, wenn Tatsachen die Annahme rechtfertigen, dass eine Straftat von erheblicher Bedeutung begangen werden soll.[123] Vorliegend war aufgrund der bisherigen Ermittlungen hiervon auszugehen. Zweck einer solchen Maßnahme darf jedoch nur die Verhinderung künftiger Straftaten sowie die Vorsorge für die Verfolgung von Straftaten[124] sein. In der Anordnung wird die Maßnahme zum einen mit der Verhinderung weiterer Straftaten begründet, zum anderen aber auch mit der Aufklärung bereits begangener Straftaten. Darüber hinaus wird die Maßnahme mit der Identifizierung von Personen der linksextremistischen Szene begründet, denen nicht unmittelbar eine Straftat vorgeworfen wird.

Da weder die Aufklärung bereits begangener Straftaten noch die Identitätsfeststellung von Personen, bei denen keine konkreten Anhaltspunkte dafür vorliegen, dass sie in naher Zukunft im überwachten Bereich Straftaten von erheblicher Bedeutung begehen werden, der vorbeugenden Bekämpfung von Straftaten oder der Vorsorge für die Verfolgung von Straftaten dienen, kann die Maßnahme nicht auf das ASOG gestützt werden. Sie konnte, soweit sie repressiver Natur war, auch nicht auf die Strafprozessordnung (StPO) gestützt

122 § 25 Abs. 3 Satz 1 ASOG
123 § 25 Abs. 1 Satz 1 Nr. 2 ASOG
124 § 1 Abs. 3 ASOG

werden, weil die hierfür erforderliche richterliche Anordnung[125] nicht vorlag. Die Durchführung einer Maßnahme im repressiven Bereich – gestützt auf eine Anordnung nach den präventiven Rechtsvorschriften – stellt insoweit im Ergebnis eine Umgehung des Richtervorbehalts dar.

Unabhängig davon war die Maßnahme auch unzulässig, soweit sie künftige Straftaten verhindern sollte. Da die Kameras nicht dazu dienten, ein präventivpolizeiliches Eingreifen zu ermöglichen, und die Bildaufzeichnungen erst nach erneuter Begehung einer Straftat ausgewertet werden sollten, war die Maßnahme nicht geeignet, die Begehung weiterer Straftaten zu verhindern. Sie war deshalb unverhältnismäßig. Zudem waren die gesetzlichen Anforderungen an die Anordnung des verdeckten Einsatzes technischer Mittel[126] im Hinblick auf die Art und Weise der Überwachung sowie den Zweck der Maßnahme nicht erfüllt, da Angaben hierzu entweder fehlten oder zu unbestimmt waren.

Dieser Verstoß gegen die gesetzlichen Datenschutzbestimmungen war zu beanstanden.[127] Gleichzeitig haben wir empfohlen, künftig bei längerfristigen Observationen durch den verdeckten Einsatz technischer Mittel bei der Anordnung und Durchführung der Maßnahme sicherzustellen, dass der Zweck der Maßnahme (Vorbeugung bzw. Bekämpfung von Straftaten) hinreichend bezeichnet ist und die jeweiligen gesetzlichen Vorgaben eingehalten werden, auch soweit sie die Verhältnismäßigkeit und Bestimmtheit der Maßnahme betreffen. Insbesondere halten wir eine dahingehende Verbesserung des Anordnungsformulars sowie eine nochmalige Unterweisung der zur Anordnung berechtigten Polizeibeamten für erforderlich.

In der Stellungnahme zu unserer Beanstandung räumte die Senatsverwaltung für Inneres und Sport ein, dass die gesetzlich vorgeschriebene Dokumentation zu Erforderlichkeit und Zweck der Maßnahme nicht hinreichend erfolgt ist. Auf die Beachtung dieser Voraussetzungen sowie auf eine entsprechende Unterweisung der anordnungsbefugten Polizeibeamten sei der Polizeipräsident zwischenzeitlich hingewiesen worden. Im Übrigen hält die Senatsverwaltung für Inneres und Sport die Durchführung der Maßnahmen jedoch weiterhin für zulässig.

125 § 163 f Abs. 3 Satz 1 und 2 StPO
126 § 25 Abs. 3 ASOG
127 § 26 BlnDSG

Die verdeckte Videoüberwachung stellt einen weitreichenden Eingriff in die Persönlichkeitsrechte der davon Betroffenen dar. Sie unterliegt daher restriktiven gesetzlichen Bestimmungen, die auch bei der Verfolgung und Verhinderung schwerwiegender Straftaten zwingend einzuhalten sind.

3.3. Wer hört mit? Einsatz von Trojanern durch Sicherheitsbehörden

Im Herbst stellte der Chaos Computer Club fest, dass einzelne Bundesländer in ihren Sicherheitsbehörden für die Überwachung von verschlüsselter Internetkommunikation (z.B. Internettelefonie) zwischen Verdächtigen eine Spähsoftware mit unzulässigen Komponenten verwendeten. Diese erlaubte das Kopieren von sonstigen auf dem Computer abgelegten Dateien oder das Fertigen von Screenshots.[128]

Zur Durchführung einer solchen Überwachungsmaßnahme, der sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), wird auf dem Endgerät der oder des Betroffenen ein Überwachungsprogramm installiert, das die laufende Kommunikation vor der Verschlüsselung erfasst und diese dann an die Behörden weiterleitet. Die Quellen-TKÜ ist ausschließlich beschränkt auf die Überwachung von Daten aus der laufenden Kommunikation, was nach der Rechtsprechung des Bundesverfassungsgerichts[129] durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen ist. Die eingesetzte Spähsoftware entsprach diesen Anforderungen nicht.

Angesichts der möglichen Eingriffsintensität und der Folgen für die Betroffenen des infiltrierten Endgerätes sowie der Verwertbarkeit der Daten als Beweismittel haben die Datenschutzbeauftragten den Gesetzgeber aufgefordert, die Zulässigkeit und die Voraussetzungen einer Quellen-TKÜ unter Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.[130]

128 Siehe 1.1

129 BVerfGE 120, 274 ff.; s. o. 1.1

130 Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011, Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten, Dokumentenband 2011, S. 15

Der Polizeipräsident hat uns mit Schreiben vom 16. Dezember mitgeteilt, er habe bisher keine Quellen-TKÜ vorgenommen und verfüge selbst über keine Anlagen zur Durchführung einer solchen Maßnahme. Hinweise auf eine Beschaffung von Anlagen zur Quellen-TKÜ durch die Berliner Polizei bei der Firma Syborg seien nicht zutreffend. Sollte durch Gerichtsbeschluss eine solche Überwachung angeordnet werden, so ist dafür die Amtshilfe einer anderen Landes- oder Bundessicherheitsbehörde notwendig. Eine solche richterliche Anordnung wie auch ihre Umsetzung muss den Vorgaben des Bundesverfassungsgerichts genügen. Ende Januar 2012 erklärte der Senator für Inneres und Sport, Frank Henkel, im Abgeordnetenhaus[131], die Berliner Polizei habe bei dem Unternehmen Syborg die Erstellung einer entsprechenden Überwachungssoftware in Auftrag gegeben.

Der Gesetzgeber sollte klare gesetzliche Regelungen schaffen, die die Telekommunikationsüberwachung auf Endgeräten begrenzen.

131 Plenarprotokoll 17/7 vom 26. Januar 2012, S. 401 f.

4. Verkehr

4.1 Touch & Travel

Das Projekt „Touch & Travel“ wurde von der Deutschen Bahn (DB) im März 2007 auf der CeBIT offiziell angekündigt. Hierbei handelt es sich um ein Vorhaben zum elektronischen Ticketing, das spontanes Fahren ermöglichen soll, da der Erwerb des Fahrscheins jederzeit über ein NFC[132]-fähiges Handy oder per App über ein Smartphone erfolgen kann. Somit ist man nicht mehr gezwungen, bereits vor Antritt der Fahrt ein Ticket zu kaufen. Nach dem Ende der Fahrt wird der Fahrpreis automatisch vom System anhand von Bewegungsdaten auf der zurückgelegten Strecke ermittelt.

Hierzu ist bei Nutzung des Angebots über die Touch & Travel-App die Zustimmung der Kundin bzw. des Kunden zur periodischen Standortbestimmung des eigenen Mobiltelefons über das Mobilfunknetz des Providers während der Fahrt erforderlich. Die Ortsbestimmung der oder des Nutzenden erfolgt anhand der durchfahrenen Funkzellen. Bei Nutzung des Touch & Travel-Angebots mit einem NFC-Handy erfolgt die Übermittlung der Standortdaten durch das Handy selbst mittels Geolokalisation per GPS. Bei beiden Verfahren ist datenschutzrechtlich bedenklich, dass anhand der erhobenen Standort- und Bewegungsdaten der Nutzenden sehr detaillierte Bewegungsprofile erstellt werden können.

Für die Datenerhebung im Zusammenhang mit Touch & Travel ist die DB-Tochter DB Mobility Logistics AG datenschutzrechtlich verantwortlich. Seit Herbst 2007 befindet sich Touch & Travel im Probebetrieb. Erste Praxistests wurden ab Oktober 2007 für die ICE-Strecke Berlin-Hannover, den Nahverkehr in Hannover, ein Teilnetz der Berliner S-Bahn sowie im gesamten städtischen Nahverkehr von Potsdam durchgeführt. Derzeit sind alle Züge der DB im Fernverkehr (ICE, IC) bereits bundesweit mit dem elektronischen Handyticket nutzbar, bisher jedoch nur für die Testkunden im Probebetrieb. Fahr-

132 Near Field Communication

karten können die Testkunden direkt per NFC-Handy, aber auch schon über die Applikation mit dem Smartphone erwerben. Bei erfolgreicher Erprobung und Freigabe des Systems durch die zuständigen Prüfbehörden ist laut DB nach Abschluss der Testphase eine deutschlandweite Einführung geplant. Die DB plante die Inbetriebnahme voraussichtlich mit Beginn des Winterfahrplans im Dezember 2011 oder zu Beginn des Jahres 2012.

Beim Angebot der DB für den bundesweiten Fernverkehr muss die Anwenderin bzw. der Anwender zuerst die DB Touch & Travel App kostenlos aus dem Apple App Store oder dem Google Android Market direkt auf das Smartphone laden. Anschließend muss sie oder er sich mit den persönlichen Daten (u.a. Name, Anschrift, Bankverbindung) registrieren. Daraufhin erhält die oder der Nutzende vom System eine Kundennummer und eine PIN zugewiesen. Mit diesen Daten kann sie oder er sich dann später beim Touch & Travel-Ticketsystem anmelden. Nach Aktivierung der Ortungsfunktion beim Smartphone können die App gestartet und die Daten aus der Registrierung (Kundennummer und PIN) eingegeben werden. Anschließend ist Touch & Travel in Berlin und Potsdam zum elektronischen Ticketerwerb nutzbar. Bei NFC-fähigen Handys aus dem ursprünglichen Testbetrieb ist auch ein Login beim Touch & Travel-System mittels eines Touchpoints möglich. Diese Touchpoints sind an allen Fernverkehrsbahnhöfen in Deutschland installiert worden. Durch die kontaktlose NFC-Technik ist ein Check-in direkt mit dem Handy möglich, indem der Fahrgast das Mobiltelefon vor den Touchpoint hält und sich somit per Datenübertragung zwischen NFC-Handy und Touchpoint am System anmeldet.

Nachdem der Fahrgast das Ende der Fahrt per Smartphone-App oder durch erneute Nutzung des Touchpoints am Zielort bekundet hat, wird der Fahrpreis anhand des aufgezeichneten Fahrweges automatisch berechnet und auf dem Handy angezeigt. Die Gesamtrechnung mit einer Übersicht über alle Fahrten erhält der Fahrgast am Monatsende und bezahlt sie per Bankeinzug. Zwischendurch kann man jederzeit seinen aktuellen Fahrtenstand samt Preisermittlung über das Internet unter www.touchandtravel.de einsehen. Laut Auskunft der DB wird möglichst immer der günstigste Fahrpreis berechnet, sofern dies technisch realisierbar ist. Rabatte durch den Einsatz einer BahnCard oder Großkundenrabatte für Firmenkunden werden ebenfalls berücksichtigt, nicht allerdings die Sparpreise.

Wenn der Fahrgast vergessen hat, sich nach Ende der Fahrt wieder abzumelden, erhält er nach etwa vier Stunden per SMS eine Erinnerung, dass er noch im System eingebucht ist. Wenn er dann feststellt, dass er sich versehentlich nicht ausgebucht hat, kann er dies unter einer kostenfreien Rufnummer der Touch & Travel-Kundenbetreuung nachholen. Tut er dies nicht, wird er bei Nutzung der Smartphone-App für weitere 13 Stunden, bei der NFC-Technik 24 Stunden lang geortet.

Unsere Forderung, das Touch & Travel-System auch anonym oder pseudonym nutzbar zu machen, sieht die DB vorerst als nicht realisierbar an. Allerdings bleibt sie in der Pflicht, weiterhin die Option einer anonymen oder pseudonymen Nutzung des Systems zu prüfen und uns über den jeweiligen Stand ihrer Bemühungen zu informieren. Die DB sagte dies zu.

Für das Touch & Travel-Verfahren muss der Kunde neben dem Abschluss eines Vertrags mit der DB Mobility Logistics AG auch ein Vertragsverhältnis mit einem Mobilfunkanbieter eingehen, der mit Touch & Travel kooperiert (derzeit Vodafone und T-Mobile). Darüber hinaus muss sich der Fahrgast mit der Erhebung und Weitergabe seiner Standortdaten durch seinen Mobilfunkanbieter an die DB oder mit der Erfassung des eigenen Standortes per Geolokalisation durch GPS-Ortung einverstanden erklären, da sonst eine Nutzung des Touch & Travel-Systems in der aktuellen Form nicht möglich ist. Die Standortdaten werden von der DB zu Bewegungsdaten weiterverarbeitet und nach maximal 90 Tagen gelöscht. Die Zulässigkeit der Verwendung der personenbezogenen Daten inklusive Standortdaten mit dem Ziel der Abrechnung geschuldeter Fahrgelder beruht auf § 4 i. V. m. § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Die Speicherdauer wurde von der DB aufgrund unserer Intervention herabgesetzt; darüber hinaus prüft die DB die Möglichkeit, die Zahl der Standortdaten weiter zu verringern, ohne die Genauigkeit der Preisberechnung zu beeinträchtigen.

Seit Juli bietet die **BVG** in Berlin ebenfalls die Nutzung von Touch & Travel für den elektronischen Ticketerwerb im Echtbetrieb an, der über eine Smartphone-App realisiert wird. Die BVG ist dabei Kooperationspartner der DB. Kundinnen und Kunden der BVG registrieren sich dazu auf der Touch & Travel-Plattform der DB. Alle Busse und Bahnen der BVG und der Berliner S-Bahn im Berliner Tarifgebiet AB sowie ebenfalls im Potsdamer Tarifgebiet AB

sind mit dem elektronischen Handyticket mittlerweile nutzbar. Tageskarten, Einzelfahrausweise und Kurzstreckentickets kann man direkt per Smartphone kaufen. Nach der Fahrt wird der Fahrpreis automatisch berechnet und auf dem Handy angezeigt. Die Fahrgeldberechnung in den genannten Nahverkehrsbetrieben berücksichtigt die Tarife für Einzelfahrscheine, Kurzstrecke oder Tageskarten, sodass am Ende eines Tages stets die preisgünstigste Variante abgerechnet wird. Ansonsten ist das Angebot identisch mit dem Touch & Travel-Angebot der DB.

Die Nahverkehrsbetriebe erheben selbst keine Kunden- oder Bewegungsdaten. Dies erfolgt ebenfalls durch die DB Mobility Logistics AG, die auch bei der Nutzung durch die Nahverkehrsbetriebe datenschutzrechtlich verantwortliche Stelle ist. Dies ist derzeit für den Fahrgast jedoch nicht immer eindeutig erkennbar; die Transparenz sollte hier erhöht werden. Wir haben deshalb auch die BVG aufgefordert, die Kundinnen und Kunden unmissverständlich über die Identität der verantwortlichen Stelle aufzuklären.

Bewertung

Das Touch & Travel-Verfahren folgt gegenwärtig einer wenig datenschutzfreundlichen Grundkonzeption, da es für die Ermittlung der Fahrpreise und für ggf. notwendige Nachweise bei Beschwerden die genaue Streckenführung für 90 Tage nachvollziehbar speichern muss. Solche Daten ermöglichen die Gewinnung von Bewegungsprofilen und könnten daher Interessen zur Zweckentfremdung auslösen. Dies ändert sich auch kaum, wenn die DB unserer Empfehlung folgt, alle Lokalisationsdaten, die während der Fahrt aufgezeichnet werden und die für die Preisermittlung und für die im Streitfall ggf. notwendigen Nachweise nicht mehr erforderlich sind, nach Abschluss der Fahrt sofort automatisch zu löschen. Aus Sicht des Datenschutzes ist daher allen anderen elektronischen Ticketing-Verfahren, die ohne minutiöse Wegstreckenaufzeichnung auskommen, der Vorzug zu geben. Dass dies geht, zeigen diverse chipkartenbasierte Ticketing-Verfahren anderer deutscher Verkehrsunternehmen, so z.B. auch das INNOS-Projekt des Verkehrsverbundes Berlin-Brandenburg (VBB).

Die fehlende anonyme oder pseudonyme Nutzungsmöglichkeit des Systems durch den Fahrgast widerspricht dem Grundgedanken des § 3a BDSG. Danach sind Datenverarbeitungssysteme an dem Ziel auszurichten, so wenig perso-

nenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen (Datensparsamkeit/Datenvermeidung). Deshalb fordert der Gesetzgeber, personenbezogene Daten zu anonymisieren, soweit dies möglich und verhältnismäßig ist. Eine datenschutzfreundliche Gestaltung des Dienstangebots (Privacy by Design and by Default) sieht jedenfalls anders aus. Die geringe Datenschutzfreundlichkeit ist nur tolerierbar, solange es sich bei Touch & Travel noch um ein Nischenprodukt handelt.

Aus datenschutzrechtlicher Sicht ist das Touch & Travel-Angebot kritisch zu beurteilen, da zu Abrechnungszwecken sowohl zahlreiche persönliche Daten als auch Bewegungsdaten des Fahrgastes erhoben werden. Zudem kann das System aktuell aufgrund konzeptioneller Mängel nur von registrierten Fahrgästen genutzt werden. Eine anonyme oder pseudonyme Nutzung ist derzeit nicht realisiert, und es ist ungewiss, ob dies künftig möglich sein wird. Die DB erhebt den Anspruch, den Datenschutz vorbildlich umzusetzen. Diesem Anspruch genügt das Touch & Travel-Verfahren bisher nicht.

4.2 Automatisierte Online-Halterauskünfte für jedermann?

Das Landesamt für Bürger- und Ordnungsangelegenheiten plante die Einführung eines Abrufverfahrens von Kfz-Halterauskünften für Privatpersonen über das Internet.

Privatpersonen können bereits aktuell Kfz-Halterauskünfte über das Internet einholen. Im Rahmen dieses Verfahrens wird die Halteranfrage manuell bearbeitet, und der Benutzer erhält eine Antwort per Briefpost. Das ist deshalb notwendig, weil eine Halterauskunft nur bekommt, wer ein berechtigtes Interesse hat. Im Rahmen der Verwaltungsmodernisierung war geplant, die Halterauskunft für Privatpersonen vollständig über ein Internetportal auszuführen. Die für die Anfrage eingegebenen Daten sollten an einen Webservice weitergeleitet werden, der automatisch ein Antwortschreiben mit der gewünschten Auskunft erstellt. Die Anfragen sollten dadurch nicht mehr von einer Sachbearbeiterin oder einem Sachbearbeiter geprüft werden müssen.

Das geplante Verfahren stellt ein automatisiertes Abrufverfahren dar. Behörden dürfen ein solches Verfahren zum Abruf personenbezogener Daten durch Dritte jedoch nur einrichten, wenn ein Gesetz dies ausdrücklich zulässt.[133] Nachdem wir festgestellt haben, dass für die automatisierte Halterauskunft keine Rechtsgrundlage vorhanden ist, hat das Landesamt für Bürger- und Ordnungsangelegenheiten von der Einführung des Verfahrens Abstand genommen.

Durch unsere frühzeitige Intervention konnte die unzulässige Einführung des automatisierten Online-Abrufverfahrens zur Abfrage von Halterauskünften abgewendet werden.

133 § 15 Abs. 1 BlnDSG

5. Justiz

5.1 Schuldnerrechte bei der Zwangsvollstreckung

Ein Petent beschwerte sich darüber, dass ein Gerichtsvollzieher im Rahmen einer Zwangsvollstreckung zur Durchsetzung eines Haftbefehls, mit dem die Abgabe einer eidesstattlichen Versicherung erzwungen werden sollte, und während der Zwangsräumung seiner Wohnung seine personenbezogenen Daten unbefugt an Dritte weitergegeben habe. Der Gerichtsvollzieher hatte, nachdem er den Petenten zur Durchsetzung des Haftbefehls nicht antraf, an der Wohnungstür eine Benachrichtigung angebracht, aus der hervorging, dass der Petent in der Vollstreckungssache nicht angetroffen worden ist, daher seine Wohnung aufgrund eines richterlichen Durchsuchungsbeschlusses kostenpflichtig von einem Schlüsseldienst zwangsweise geöffnet wurde und neue Schlüssel beim Polizeirevier abgeholt werden können. Der Gerichtsvollzieher wurde bei der späteren Zwangsräumung von einem Spediteur begleitet, der für ihn zu entsorgende Sachen des Petenten, u.a. dessen Kontoauszüge, nach zu verwahrenden Papieren durchsah.

Der Gerichtsvollzieher erklärte, die Form der Bekanntgabe sei erforderlich gewesen, um einer Herbeiholung der Polizei wegen vermuteten Einbruchs vorzubeugen. Zudem sei die Nutzung des Briefkastens wenig sinnvoll gewesen, da der Petent bereits mehrfach derartige Mitteilungen ignoriert hatte.

Das Anbringen der Nachricht an der Wohnungstür war unzulässig. Die Nachricht war für jedermann, der an der Tür vorbeiging, sichtbar. Die personenbezogenen Daten des Petenten wurden voraussichtlich auf diese Weise an Dritte übermittelt. Eine solche Übermittlung bedarf einer besonderen Rechtsvorschrift oder einer Einwilligung des Betroffenen.[134] Beides lag hier nicht vor. Die Begründung, dass einem mutmaßlichen Polizeieinsatz vorgebeugt werden sollte, ist nicht nachvollziehbar, da für alle sichtbar ein neues Schloss eingebaut wurde. Selbst wenn der Schuldner gerichtliche Schreiben in seinem Brief-

134 § 6 Abs. 1 Satz 1 BlnDSG

kasten ignoriert (also auf sie nicht reagiert) hat, bedeutet dies nicht, dass er sie nicht zur Kenntnis genommen hat. Auch wenn kein Dritter die Nachricht an der Wohnungstür zur Kenntnis genommen hat und daher keine Übermittlung von Daten stattfand, hat der Gerichtsvollzieher zumindest gegen die Pflicht verstoßen, technische und organisatorische Maßnahmen zu treffen, um zu verhindern, dass Unbefugte personenbezogene Daten zur Kenntnis nehmen können.[135] Wir haben daher einen Mangel festgestellt und den Gerichtsvollzieher aufgefordert, zukünftig derartige Benachrichtigungen nur dem jeweils Betroffenen zugänglich zu machen.

Die Durchsicht der Unterlagen durch den vom Gerichtsvollzieher beauftragten Spediteur war ebenfalls unzulässig. Grundsätzlich gelten für einen Spediteur die Regelungen des Bundesdatenschutzgesetzes, wonach die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.[136] Diese Bedingungen waren hier nicht erfüllt. Soweit er für den Gerichtsvollzieher die personenbezogenen Daten des Petenten im Auftrag verarbeitet hat, gelten die Regelungen des Berliner Datenschutzgesetzes. Danach ist es u.a. erforderlich, dass der Gerichtsvollzieher als Auftraggeber zur Verarbeitung der personenbezogenen Daten des Petenten befugt ist[137]. Die Regelungen zur Zwangsvollstreckung zur Erwirkung der Herausgabe von unbeweglichen Sachen erlauben grundsätzlich keine Durchsicht von Unterlagen eines Schuldners.[138] Lediglich bei großen Mengen von Abfall kann der Müll für den Schuldner entsorgt werden[139] und hierfür im Interesse des Schuldners eine Durchsicht nach wichtigen Unterlagen angebracht sein. Für uns war nicht eindeutig ersichtlich, ob hier eine solche Ausnahmesituation vorlag. Geht man jedoch davon aus, bestand für den Gerichtsvollzieher eine Befugnis zur Durchsicht der persönlichen Unterlagen des Petenten. Eine Übertragung der Aufgabe auf den Spediteur war aber schon deshalb unzulässig, weil der Gerichtsvollzieher mit diesem keinen schriftlichen Auftragsdatenverarbeitungsvertrag unter Regelung der gesetzlich vorgegebenen Einzelheiten[140] abgeschlossen hat.

135 § 5 Abs. 1 BlnDSG
136 § 4 Abs. 1 BDSG
137 Vgl. § 3 Abs. 1 Satz 1 i. V. m. § 6 Abs. 1 Satz 1 BlnDSG
138 Vgl. § 885 Abs. 2 bis 4 ZPO
139 § 887 ZPO
140 § 3 Abs. 1 Satz 3 BlnDSG

Wir haben daher auch insoweit einen Mangel festgestellt und den Gerichtsvollzieher aufgefordert, zukünftig dafür Sorge zu tragen, dass weder er noch eine von ihm beauftragte Person oder Stelle im Rahmen der Zwangsräumung einer Wohnung Unterlagen durchsehen, aus denen sich personenbezogene Daten des Schuldners oder Dritter ergeben. Soweit ausnahmsweise große Mengen Abfall zu behandeln sind, sollte die Aussortierung von entsprechenden Unterlagen vom Gerichtsvollzieher eigenhändig durchgeführt werden.

Gerichtsvollzieher haben sicherzustellen, dass Informationen über Vollstreckungsmaßnahmen nicht rechtswidrig an Dritte gelangen.

5.2 Veröffentlichung von Richterdaten im Internet

Der Datenschutzbeauftragte eines Gerichts machte uns darauf aufmerksam, dass eine Privatperson auf ihrer Internetseite personenbezogene Daten von Richterinnen und Richtern Berlins und anderer Bundesländer veröffentlicht. Der Betreiber der Internetseite möchte mit der Veröffentlichung dieser Daten Vätern insbesondere in gerichtlichen Familienstreitigkeiten beratend zur Seite stehen.

Die Daten sind größtenteils dem Handbuch der Justiz entnommen, das seit Jahren in nichtelektronischer Form als Nachschlagewerk der Justiz Informationssuchenden vom Deutschen Richterbund zur Verfügung gestellt wird. Es enthält u.a. Namen, Geburtsdaten und Dienstalter von Richterinnen und Richtern. Die Betroffenen haben in diese Form der Datenübermittlung schriftlich eingewilligt. Neben diesen Daten werden auf der Internetseite Mutmaßungen über den Familienstand und Verwandtschaftsverhältnisse einzelner Richterinnen und Richter angestellt. Weiterhin enthalten die veröffentlichten Datensätze teilweise Angaben zu sozialen Aktivitäten der Betroffenen. Alle vorgenannten Daten sind über Suchmaschinen wie Google weltweit auffind- und abrufbar.

Die Datenübermittlung ist in dieser Form unzulässig, da die Betroffenen hierin nicht eingewilligt haben und sie nicht auf eine Rechtsgrundlage gestützt

werden kann.[141] Es ist bereits sehr zweifelhaft, ob die Weitergabe von Informationen über (vermutete) Verwandtschaftsverhältnisse, Familienstände und soziale Aktivitäten von Richterinnen und Richtern für die Beratung von Vätern in Familienrechtsstreitigkeiten relevant ist. Jedenfalls überwiegen die schutzwürdigen Interessen der betroffenen Personen an dem Ausschluss der Verarbeitung ihrer Daten in dieser Form, weil hierbei eine Profilbildung erfolgt, die geeignet ist, in unangemessener Weise auf die Betroffenen privaten und gesellschaftlichen Druck auszuüben sowie Einfluss auf deren berufliche und außerberufliche Betätigungen zu nehmen. Da die Betroffenen aufgrund der weltweiten Abrufbarkeit der Informationen nicht mehr erkennen können, wer welche Kenntnisse über sie hat, besteht die Gefahr, dass sie sowohl als Privatpersonen als auch in ihren richterlichen Ämtern nicht mehr unvoreingenommen handeln können.

Wir haben daher den Betreiber der Interseite aufgefordert, keine Daten der Richterschaft zu deren mutmaßlichen Verwandtschaftsverhältnissen, Familienständen sowie nicht allgemein bekannten sozialen Aktivitäten zu veröffentlichen. Dieser Aufforderung ist der Betreiber nicht nachgekommen; deshalb haben wir eine Anordnung entsprechenden Inhalts erlassen. Hiergegen hat der Inhaber der Internetseite Klage bei dem Verwaltungsgericht Berlin erhoben, über die bislang noch nicht entschieden wurde.

Auch Personen in öffentlichen Ämtern haben ein Recht auf Privatsphäre. Die Gefahr einer Verletzung dieses Rechts ist bei Veröffentlichung von Datensätzen im Internet, die über Suchmaschinen leicht auffindbar und weltweit einsehbar sind, besonders groß.

5.3 Einführung der elektronischen Fußfessel

Aufgrund des Urteils des Europäischen Gerichtshofs für Menschenrechte zur nachträglichen Sicherungsverwahrung[142] hat der Gesetzgeber die gesetzlichen Bestimmungen hierzu neu geregelt. Diese Gelegenheit wurde auch

141 Insbesondere kann sie nicht auf § 28 Abs. 1 Satz 1 Nrn. 2, 3 BDSG gestützt werden.
142 Urteil vom 17. Dezember 2009, Nr. 19359/04

dazu genutzt, führungsaufsichtsrechtliche Befugnisse zu erweitern. Insbesondere wurde das Instrumentarium der elektronischen Aufenthaltsüberwachung („Fußfessel“) zur Verbesserung der Kontrolle aufenthaltsbezogener Weisungen eingeführt.[143]

Rechtsgrundlage für die Erhebung und Verarbeitung personenbezogener Daten bei der Durchführung einer elektronischen Aufenthaltsüberwachung bildet der neue § 463 a Abs. 4 StPO. Danach sind die Erhebung und Speicherung aller Aufenthaltsdaten einschließlich der Daten über eine Beeinträchtigung der Erhebung erlaubt. Lediglich innerhalb der Wohnung dürfen mit Verweis auf den Kernbereich privater Lebensführung keine über den Umstand der Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden, soweit dies technisch möglich ist; anderenfalls dürfen solche Daten nicht verwertet und müssen umgehend gelöscht werden. Die Weiterverarbeitung der Daten ist an bestimmte, abschließend aufgezählte, eng begrenzte Zwecke gebunden. Die Daten sind gegen unbefugte Kenntnisnahme zu sichern und – soweit kein Weisungsverstoß festgestellt wird – nach zwei Monaten zu löschen.

Zur Art der elektronischen Aufenthaltsüberwachung sind mit Verweis auf die Offenheit für neue technische Entwicklungen keine bestimmten Regelungen getroffen worden. In der Begründung des Gesetzentwurfs wird festgestellt, dass es in Deutschland bislang noch keine praktischen Erfahrungen gebe, weshalb es sich empfehlen könne, zunächst in Pilotprojekten zu klären, welche technischen Vorkehrungen zu treffen und welche Geräte – mit welchen Messgenauigkeiten – im Einzelnen einzusetzen sind, um die Überwachung praktikabel zu machen[144].

Diese Empfehlung der Erprobung technischer Systeme in einzelnen Pilotprojekten war aufgrund der seit Inkrafttreten des Gesetzes Ende 2010 flächendeckenden Gültigkeit der neuen Weisungsbefugnisse praktisch nicht umsetzbar, weil die Regelung zur elektronischen Fußfessel kurz vor Verabschiedung in den Gesetzestext aufgenommen worden war. Die richterliche Anordnung einer elektronischen Aufenthaltsüberwachung muss bei Vorliegen der entsprechenden Voraussetzungen ortsunabhängig von der jeweils zuständigen Führungs-

143 § 68 b Abs. 1 Satz 1 Nr. 12 Strafgesetzbuch
144 BT-Drs. 17/3403, S. 19

aufsichtsstelle sofort umgesetzt werden. Die technische Entwicklung passender Systeme verläuft somit derzeit zwangsläufig parallel zu den Weisungsdurchführungen, was erhebliche datenschutzrechtliche und praktische Probleme mit sich bringt.

Berlin hat sich zusammen mit der Mehrheit der Bundesländer dafür entschieden, die Durchführung entsprechender gerichtlicher Auflagen gemeinsam zu organisieren. Hierzu soll die aufgrund eines Modellversuchs in Hessen vorhandene technische Infrastruktur bei der Hessischen Zentrale für Datenverarbeitung genutzt und erweitert werden. Daneben wurde eine Gemeinsame elektronische Überwachungsstelle der Länder in Hessen eingerichtet. Die Zusammenarbeit soll in einem Staatsvertrag sowie einer Verwaltungsvereinbarung zur technischen und organisatorischen Umsetzung geregelt werden.

Der Einsatz der elektronischen Aufenthaltsüberwachung hat so zu erfolgen, dass die Rechte Betroffener und Dritter bestmöglich geschützt werden.

5.4 Zu praxisnahe Ausbildung künftiger Juristen

Aus der Praxis

Sehr erstaunt war ein Bürger, als er seinen Namen bei einer Suchmaschine im Internet eingab und dort eine Strafanzeige lesen konnte, die er vor etwa zwanzig Jahren bei der Polizei erstattete. Lediglich der Ort, an dem sich das Geschehen abspielte, stimmte nicht mit dem realen Ort überein.

Der Text war Teil einer Klausur, die im Rahmen eines Internetklausurenkurses für den juristischen Vorbereitungsdienst in Berlin durch das Gemeinsame Juristische Prüfungsamt der Länder Berlin und Brandenburg (GJPA) veröffentlicht wurde. Der Präsident des GJPA erklärte, dass Klausuren im Zweiten Staatsexamen zur Förderung einer praxisnahen Prüfung regelmäßig aus Originalakten entwickelt werden. Gewöhnlich werden hierbei alle personenbezogenen Daten anonymisiert. Bei der beanstandeten Klausur handele es sich um eine ehemalige Examensklausur eines anderen Bundeslandes, die durch die Ausbildungsabteilung aktualisiert worden sei. Diese sei davon ausgegangen, dass in der Vorlage wie üblich keine Originaldaten Verwendung gefunden hätten. Eine

weitere Aufklärung des Sachverhalts sei nicht möglich, weil das Bundesland, in dem die Klausur ursprünglich konzipiert worden sei, aufgrund der langen Zeit, die seit der Erstellung vergangen sei, keine Unterlagen mehr habe, aus denen sich der Vorgang der Erstellung rekonstruieren lasse.

Nach Bekanntwerden der Veröffentlichung der personenbezogenen Daten wurde die beanstandete Klausur umgehend aus dem aktuellen Internetklausurenkurs entfernt. Nachdem festgestellt wurde, dass der Text auch im Onlinearchiv des Internetklausurenkurses abrufbar war, wurde er dort ebenfalls unverzüglich gelöscht. Das GJPA informierte die anderen Prüfungsämter über den Vorfall.

Klausuren der juristischen Prüfungsämter sind sorgfältig zu anonymisieren.

6. Finanzen

6.1 Übertragung von Forderungen auf private Inkassounternehmen

Aus der Praxis

Nachdem wir uns bereits 2009[145] allgemein mit der Problematik der Übertragung von öffentlichen Forderungen auf private Inkassounternehmen beschäftigt hatten, wurden wir zu Beginn des Jahres 2011 durch Zeitungsmeldungen darauf aufmerksam, dass der Bezirk Marzahn-Hellersdorf konkret plane, Zahlungsrückstände durch private Unternehmen einziehen zu lassen. Später bat uns das Abgeordnetenhaus, den Bezirk bei seinem Vorhaben zu beraten, damit ein entsprechendes Verfahren auch in anderen Bezirken angewandt werden könne.[146]

Der Einzug von offenen Forderungen der öffentlichen Hand durch ein damit beauftragtes Privatunternehmen setzt grundsätzlich voraus, dass dem Unternehmen Daten der Schuldnerin oder des Schuldners zur Verfügung gestellt werden. Ist dies eine natürliche Person, handelt es sich um personenbezogene Daten, die dem Datenschutz unterliegen. Wird das private Inkassounternehmen von der öffentlichen Stelle (weisungsgebunden) lediglich mit Hilfsleistungen im Vorfeld der eigentlichen Vollstreckung beauftragt und erlangt es dabei keine genaue Kenntnis über das konkrete Schuldverhältnis, ist die Angelegenheit datenschutzrechtlich relativ unproblematisch. Das Unternehmen wird in diesem Fall als Verwaltungshelfer für die öffentliche Stelle im Wege der Auftragsdatenverarbeitung tätig. Die Vollstreckungsaufgabe selbst verbleibt bei der öffentlichen Stelle, das Inkassobüro erbringt lediglich Unterstützungsleistungen (z.B. Führung der Korrespondenz, Überprüfung der Bonität der Schuldner, Adressenermittlung, Vermittlung von Ratenzahlungsvereinbarungen als Bote des Auftraggebers). Die öffentliche Stelle ist weiterhin Daten verarbeitende Stelle und für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Anders verhält es sich, wenn dem Privatunternehmen das Inkasso der Forderung (durch echtes oder unechtes Factoring) vollständig übertragen

145 JB 2009, 6.1
146 Vgl. Anhang 1

werden soll. Bei der Weitergabe von Schuldnerdaten durch die öffentliche Stelle an das Inkassounternehmen im Rahmen einer derartigen Funktionsübertragung handelt es sich um eine Datenübermittlung, die datenschutzrechtlich nur aufgrund einer ausdrücklichen Erlaubnisnorm zulässig ist.

Für die Übertragung von öffentlich-rechtlichen Forderungen durch die öffentliche Hand auf ein Privatunternehmen gibt es derzeit in Berlin keine derartige Rechtsgrundlage. Während der Landesgesetzgeber für einige dieser Forderungen eine Regelung (z.B. in der Landeshaushaltsordnung) schaffen könnte, sind wesentliche Bereiche des öffentlichen Forderungsmanagements (z.B. im Steuer- und Sozialbereich) in Bundesgesetzen geregelt. Landesrechtliche Sonderwege (z.B. zur Einschränkung des Steuergeheimnisses und des Sozialdatenschutzes) sind hier ausgeschlossen. Dagegen können privatrechtliche Forderungen von öffentlichen Stellen, die i. S. d. § 2 Abs. 3 BlnDSG am Wettbewerb teilnehmen, an private Inkassounternehmen abgetreten und veräußert werden.[147] Die damit einhergehende Übermittlung von personenbezogenen Schuldnerdaten kann grundsätzlich - ebenso wie bei privaten Unternehmen - auf die Bestimmungen des Bundesdatenschutzgesetzes gestützt werden.[148] Das Bezirksamt Marzahn-Hellersdorf hat diese Vorgaben akzeptiert. In diesem Rahmen können auch andere Bezirke private Inkassounternehmen datenschutzgerecht beauftragen.

Die Übermittlung von personenbezogenen Schuldnerdaten an private Inkassounternehmen zur Einziehung privatrechtlicher Forderungen von öffentlichen Stellen, die am Wettbewerb teilnehmen, ist datenschutzrechtlich grundsätzlich zulässig. Ansonsten würden öffentliche Wettbewerbsunternehmen gegenüber privaten Konkurrenten benachteiligt.

147 Z. B. Forderungen von Mietkosten, Betriebskosten, Nutzungsentschädigungen, Pacht (im Bereich der Wohnungs-, Gebäude und Grundstücksverwaltung); nicht dagegen z.B. Gebühren für die Genehmigung von Veranstaltungen

148 Vgl. § 2 Abs. 3 BlnDSG

6.2 Eine Steuerprüfung im Urlaub

Aus der Praxis

Der Eigentümer eines Gehöfts in Ostbevern, bestehend aus mehreren z. T. vermieteten Gebäuden, teilte uns mit, dass sich der zuständige Mitarbeiter des Finanzamts Schöneberg während seines Privaturlaubs in Ostbevern Zutritt zum Grundstück verschafft, das Objekt besichtigt und den Mieter zu der Steuerangelegenheit befragt habe. Dabei habe er auch Mietverträge einsehen wollen, obwohl diese Unterlagen dem Finanzamt bereits in Kopie vorlagen. Weder im Vorfeld noch im Nachgang der Maßnahme sei der Eigentümer vom Finanzamt darüber informiert worden.

Die Finanzbehörden haben die Steuern festzusetzen und zu erheben, die nach den gesetzlichen Bestimmungen entstanden sind und geschuldet werden.[149] Dabei ist der entscheidungserhebliche Sachverhalt von Amts wegen zu ermitteln.[150] Über Art und Umfang der Sachverhaltsaufklärung haben die Finanzbehörden nach pflichtgemäßem Ermessen zu entscheiden[151]; gesetzliche Vorgaben für die Ermessensausübung sind allein die „Umstände des Einzelfalls". Beteiligte und Dritte haben bei der Aufklärung des steuerrelevanten Sachverhalts Mitwirkungspflichten.[152] Den Finanzbehörden steht insofern auch in der Auswahl der heranzuziehenden Erkenntnisquellen ein Ermessen zu. Sie haben jedoch unter dem Gesichtspunkt der Verhältnismäßigkeit die Aufklärungsmaßnahmen zu ergreifen, die die Beteiligte oder den Beteiligten am wenigsten belasten, den größten Erfolg versprechen und für alle Betroffenen zumutbar sind. Unter dem Gesichtspunkt der Verhältnismäßigkeit ist zur Aufklärung des Sachverhalts grundsätzlich mit dem mildesten Mittel zu beginnen, nämlich der Aufforderung an den Beteiligten, Auskunft zu erteilen.[153]

Nach Auffassung des Finanzamts Schöneberg führte die Auskunftserteilung durch den Petenten nicht zum gewünschten Erfolg. Das Finanzamt ist daher seiner Pflicht nachgekommen, den fraglichen Sachverhalt abschließend aufzuklären. Dabei ist es auch grundsätzlich unschädlich, dass sich der zuständige

149 § 85 AO
150 § 88 AO
151 § 5 AO
152 §§ 90, 93 AO
153 § 93 Abs. 1 S. 3 AO

Finanzbeamte zurzeit der Beweisermittlung im Urlaub befand. Eine Ermittlung von Amts wegen ist auch in solchen Fällen grundsätzlich zulässig. Wie das Finanzamt bestätigt hat, handelte der zuständige Beamte in seiner Funktion als Finanzbeamter und nicht als Privatmann, indem er seinen Urlaub zum Zwecke der Beweisermittlung kurzzeitig unterbrochen hat.

Die vom Finanzamt zur Aufklärung des Sachverhalts durchgeführten Maßnahmen in Form der Befragung des Mieters sowie der Inaugenscheinnahme der Örtlichkeit waren im konkreten Fall jedoch unverhältnismäßig. Folge des Verhältnismäßigkeitsgrundsatzes ist auch, dass der Beteiligte von der beabsichtigten Befragung eines Dritten – soweit der Ermittlungszweck dadurch nicht gefährdet wird – in Kenntnis gesetzt wird, um diese Form des Auskunftsersuchens gegebenenfalls abwenden und damit verhindern zu können, dass seine steuerlichen Verhältnisse Dritten bekannt werden. Das Finanzamt hatte den Petenten weder im Vorfeld noch im Nachgang über die Befragung des Mieters unterrichtet. Da die Befragung des Mieters nicht das für den Petenten mildeste Mittel darstellte, war die Maßnahme des Finanzamtes unverhältnismäßig.

Vor allem aber hat der Finanzbeamte durch die Mitteilung von steuerlich relevanten Daten an den Mieter der Immobilie das Steuergeheimnis des Petenten verletzt. Sachverständigen, Zeugen und auskunftspflichtigen Dritten dürfen die Verhältnisse des Betroffenen offenbart werden, soweit dies notwendig ist, damit diese Personen sachgerecht ihren Verpflichtungen nachkommen können. Der Begriff "Verhältnisse" umfasst alle persönlichen und wirtschaftlichen Umstände, die mit einer bestimmten Person in Zusammenhang stehen. Alles, was aus dem persönlichen, wirtschaftlichen, privaten oder öffentlichen Bereich einer Person bekannt geworden ist, wird vom Steuergeheimnis geschützt. Auf die steuerliche Relevanz der Daten kommt es nicht an. Die Tatsache, dass der Petent Eigentümer und Vermieter des „Gehöfts" ist, lässt ebenso Rückschlüsse auf seine „Verhältnisse" zu wie die Tatsache, dass er Beteiligter in einem Steuerfestsetzungsverfahren ist.

Wir haben in der Angelegenheit gegenüber der Senatsverwaltung für Finanzen einen datenschutzrechtlichen Mangel festgestellt. Da es sich um einen Einzelfall handelte, in dem der Mitarbeiter des Finanzamtes zudem davon ausging, im Interesse des Petenten (Abschluss des Einspruchsverfahrens) zu handeln, haben wir von einer Beanstandung abgesehen.

Personenbezogene Daten sind grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben. Dies gilt auch bei Ermittlungen zur Feststellung des steuerrelevanten Sachverhalts. Nur bei erheblichen Gründen darf von diesem Grundsatz abgewichen werden.

6.3 Patientenbefragung durch das Finanzamt

Aus der Praxis

Ein Zahnarzt teilte uns mit, dass das Finanzamt bei einer Betriebsprüfung festgestellt habe, dass die Praxisgebühren, die er gegenüber der Kassenärztlichen Vereinigung (KZV) angegeben hatte, nicht in der Buchführung erfasst waren. Zur Begründung erklärte der Zahnarzt, er habe die Praxisgebühr aus ökonomischen Gründen nicht von seinen Patienten eingezogen. Zur Glaubhaftmachung seiner Behauptung habe das Finanzamt von ihm die Vorlage von Listen mit Patientendaten gefordert. Daraufhin habe sein Steuerberater dem Finanzamt für die Jahre 2005, 2006 und 2007 Listen mit jeweils zwischen 762 und 900 Patientennamen sowie Angaben über deren Geburtsdatum und Telefonnummer übergeben. Aus den Listen habe das Finanzamt stichprobenartig 33 Patientinnen und Patienten ausgewählt und diese um Auskunft zur Patienteneigenschaft, zur gesetzlichen Versicherungspflicht und um Angaben zur Zahlung der Praxisgebühr gebeten.

Im Rahmen der Amtsermittlung haben die Finanzbehörden den für die Besteuerung maßgeblichen Sachverhalt zu ermitteln. Sie haben dabei alle Erkenntnisquellen zu nutzen und entscheiden nach pflichtgemäßem Ermessen über Art und Umfang der Sachverhaltsaufklärung. Sie dürfen eigene Ermittlungen anstellen oder das ihr vorliegende Datenmaterial anderer Behörden (z.B. Kontrollmitteilungen) und andere Beweismittel nutzen. Zunächst sollen die Finanzbehörden versuchen, die zur Aufklärung des Sachverhalts notwendige Auskunft von dem Steuerpflichtigen selbst zu erlangen. Ein Auskunftsersuchen an Personen, die nicht an dem Besteuerungsverfahren beteiligt sind, soll erst ergehen, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht.[154]

154 Dazu ausführlicher unter 6.2

Grundsätzlich bedarf es für das Tätigwerden der Finanzbehörden eines hinreichenden Anlasses. Ermittlungen „ins Blaue hinein“ sind unzulässig. Eine Ermittlung „ins Blaue hinein“ liegt dann nicht vor, wenn die Finanzbehörden im Rahmen ihrer Tätigkeit – sei es aufgrund konkreter Momente, sei es aufgrund allgemeiner Erfahrung – zu dem Ergebnis gelangt sind, die Auskünfte eines Dritten könnten zur Aufdeckung steuererheblicher Tatsachen führen. Zu den steuerlich erheblichen Tatsachen zählt alles, was die finanzbehördlichen Entscheidungen in einem steuerrechtlichen Verwaltungsverfahren beeinflussen kann. Für die notwendige Prognoseentscheidung darf auch auf eine branchenspezifische Erfahrung zurückgegriffen werden. Vorliegend kann die allgemeine Erfahrung der Steuerverwaltung, dass es im Bereich niedergelassener Ärztinnen und Ärzte mehr als unüblich ist, die Praxisgebühr von den Patienten aus ökonomischen Gründen nicht einzubehalten, als ausreichend für weitere Ermittlungen in Form von Auskunftsersuchen an Dritte angesehen werden.

Nach Mitteilung der Senatsverwaltung für Finanzen diente die Befragung der Patientinnen und Patienten ausschließlich dem Zweck, die Glaubwürdigkeit der Behauptung des Einnahmeverzichts durch den Petenten zu hinterfragen. Um den Umgang mit der Praxisgebühr in der Zahnarztpraxis des Petenten festzustellen, wäre eine Befragung der dort tätigen Mitarbeiterinnen und Mitarbeiter geeignet gewesen. Diese wären nach § 93 Abs. 1 AO auch zur Erteilung der entsprechenden Auskünfte verpflichtet gewesen. Eine Befragung des Personals wäre im Verhältnis zu dem Auskunftsersuchen an die Patienten angesichts der damit verbundenen Durchbrechung der ärztlichen Schweigepflicht auch das mildere Mittel gewesen. Letztlich war es somit nicht erforderlich, die Patienten danach zu befragen, ob in der Arztpraxis des Petenten tatsächlich auf die Einziehung der Praxisgebühr verzichtet wurde. Darüber hinaus war die Erhebung von personenbezogenen Daten über mehrere tausend Patientinnen und Patienten zur Auswahl einer Stichprobe von 33 Personen für die Auskunftserteilung unverhältnismäßig.

Wir haben die unverhältnismäßige Erhebung von Patientendaten gegenüber der Senatsverwaltung für Finanzen beanstandet. Diese hat mitgeteilt, dass sie die Berliner Finanzämter auf die Besonderheiten bei der Prüfung von Berufsgeheimnisträgern und die Möglichkeit der Befragung von Beschäftigten hinweisen werde. Gleichzeitig werde sie die Finanzämter bitten, zukünftig die Datenerhebung auf das unbedingt notwendige Maß zu beschränken.

Die Finanzämter haben anlässlich von Betriebsprüfungen in Arztpraxen die Geheimnisträgerfunktion des zu überprüfenden Arztes nach § 102 AO hinreichend zu würdigen. Bei Auskunftsersuchen der Finanzämter an Patientinnen bzw. Patienten ist der Grundsatz der Erforderlichkeit strikt zu beachten, und es sind Verfahren der Pseudonymisierung bzw. Anonymisierung zu verwenden.

6.4 Aufbewahrung nach § 147 AO

Aus der Praxis

Ein Petent teilte uns mit, dass ein Parkgaragenunternehmen Daten zu seiner Person weiter speichern würde, obwohl er dessen Zahlungsaufforderung fristgerecht nachgekommen sei. Auf Nachfrage bestätigte das Unternehmen, dass tatsächlich weiterhin Angaben zur Person des Petenten (Name, Vorname, Kfz-Kennzeichen, Fahrzeughersteller, Fahrzeugfarbe, Kontonummer, Bankleitzahl) gespeichert werden, obwohl der eigentliche Zweck für die Datenspeicherung – Abwicklung des Vertragsverhältnisses – entfallen sei. Begründet wurde die weitere Datenspeicherung u.a. mit der gesetzlichen Aufbewahrungspflicht aus der Abgabenordnung.

Personenbezogene Daten sind zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.[155] Soweit der Löschung gesetzliche Aufbewahrungspflichten entgegenstehen, ist eine Sperrung der Daten vorzunehmen.[156]

§ 147 Abs. 3 Satz 1 AO sieht eine gesetzliche Aufbewahrungspflicht von zehn Jahren für Bücher, Aufzeichnungen und Buchungsbelege vor. Ohne diese Pflicht zur Aufbewahrung wären die Finanzbehörden weder in der Lage, sich einen Überblick über die Vermögenslage und einzelne Geschäftsvorfälle zu verschaffen[157], noch könnte eine Außenprüfung ohne die Vorlage von Aufzeichnungen sinnvoll durchgeführt werden.[158] Eine Nachprüfbarkeit der ordnungsgemäßen Besteuerung wäre ohne Dokumentation der Geschäftsvorfälle

155 § 35 Abs. 2 Satz 2 Nr. 3 BDSG
156 § 35 Abs. 3 Nr. 1 BDSG
157 § 145 Abs. 1 Satz 1 AO
158 § 245 Abs. 2 AO

nicht möglich. Sowohl das Steuerrecht als auch das Handelsrecht gehen von dem Grundsatz aus, dass Aufzeichnungen vollständig vorgenommen werden müssen.[159] Diesen Vorgaben lässt sich jedoch nicht entnehmen, dass die Ausführungen in jedem Fall personalisiert gefasst werden müssen. Sofern der Zweck der Buchführung ohne eine Personalisierung erreicht werden kann, muss diese bereits im Hinblick auf das Recht auf informationelle Selbstbestimmung der Betroffenen und in Anbetracht der langen Speicherfrist unterbleiben.

Eine Ausnahme besteht insofern bereits bei Bargeschäften. Eine Einzelaufzeichnung der baren Betriebseinnahmen im Einzelhandel ist nach der Rechtsprechung des Bundesfinanzhofs unter dem Aspekt der Zumutbarkeit nicht erforderlich, sofern Waren von geringem Wert an eine Vielzahl nicht bekannter und auch nicht feststellbarer Personen verkauft werden. Besteht also bei den Bargeschäften mit einem geringen Geldvolumen keine zwingende Notwendigkeit einer Personalisierung, stellt sich die Frage, warum dieses für andere (Massen-) Geschäfte nicht ebenfalls gelten sollte. Die präzise (namentliche) Benennung einer Kundin oder eines Kunden ist zumindest bei einem geringen Betrag nicht zwingend notwendig für die Erfüllung des Zwecks der Buchführung.

Auch das „Belegprinzip“ steht dem nicht entgegen. Danach gehört es zur vollständigen und richtigen Buchung bzw. Aufzeichnung, dass jede Eintragung durch einen Beleg ergänzt wird. Für Betriebsausgaben und Werbungskosten kleineren Umfangs, für die üblicherweise kein Beleg erteilt wird, müssen jedoch Eigenbelege gefertigt werden. In Anbetracht dieses Prinzips ist es grundsätzlich auch möglich, bei Buchungen kleineren Umfangs, für die Belege vorhanden sind, in der Buchführung einen entsprechenden Beleg mit einer Anonymisierung zu erstellen, sodass eine Löschung erfolgen kann, wenn lediglich auf diese Weise die Verhältnismäßigkeit im Hinblick auf das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt werden kann; zumal der Beleg nur den zu erfassenden Geschäftsvorfall, den zu buchenden Betrag, den Zeitpunkt des Geschäftsvorfalls sowie die Autorisation des Geschäftsvorfalls durch die dazu Berechtigten erkennen lassen muss. Eine Nennung weiterer Personen, die an dem Geschäftsvorfall beteiligt waren, ist nicht zwingend notwendig.

159 § 146 Abs. 1 AO, § 239 Abs. 2 HGB

Die Senatsverwaltung für Finanzen hält dagegen eine Buchführung, bei der die einzelnen Geschäftsvorfälle nicht Personen zuzuordnen sind, für nicht ordnungsgemäß. Eine (ggf. nachträgliche) Anonymisierung von Geschäftsvorfällen sei mit dem Verifikationsprinzip und dem Gebot der Gleichmäßigkeit der Besteuerung nicht vereinbar, da eine umfassende Überprüfung der Buchführung und eine Beteiligung am allgemeinen wirtschaftlichen Geschäftsverkehr erheblich erschwert bzw. gänzlich unmöglich wird.

Die Personalisierung aller Belege ist keine zwingende Voraussetzung für eine ordnungsgemäße Buchführung. Im Bereich von Alltagsgeschäften des Einzelhandels, der Gastronomie oder der Parkraumbewirtschaftung ist die Bedeutung der Personenbeziehbarkeit von Geschäftsvorfällen nicht offenkundig. Die weitere Speicherung von personenbezogenen (Kunden-)Daten ist hier nicht erforderlich. Der Grundsatz der Verhältnismäßigkeit als Teil des Rechtsstaatsprinzips nach Art. 20 Abs. 3 GG zwingt dazu, diese Daten nicht nach § 35 Abs. 3 Nr. 1 BDSG zu sperren, sondern zu löschen.

7. Sozialordnung

7.1. Sozial- und Jugendverwaltung

7.1.1 Brief des Regierenden Bürgermeisters und des Bildungssenators an Kita-Eltern

Aus der Praxis

Im Januar erhielten rund 55.000 Eltern von Kindern in Kindertagesstätten (Kitas) einen gemeinsamen Brief des Regierenden Bürgermeisters und des Senators für Bildung, Wissenschaft und Forschung. Darin wurde für die zu Jahresbeginn eingeführte Beitragsfreiheit der letzten drei Kita-Jahre vor dem Schulbesuch geworben. Die Eltern wurden gebeten, auch im Verwandten- und Bekanntenkreis für den Besuch einer Kita zu werben. Ein Mitglied des Abgeordnetenhauses bat uns um Klärung, woher die Namen und Adressdaten der Eltern stammten und ob deren Verwendung mit dem Datenschutzrecht in Einklang stand. Der Senator für Bildung, Wissenschaft und Forschung teilte uns daraufhin mit, die Daten seien aus den Stammdaten der Verträge mit den Kitas herausgefiltert worden. Dies stehe im Einklang mit den rechtlichen Vorgaben.

Die für die Kitas zuständigen bezirklichen Jugendämter haben die Eltern in allen Fragen der Beantragung einer Tagesbetreuung für ihre Kinder zu beraten. Sie erheben zur Erstellung der sog. Kita-Gutscheine eine Vielzahl von personenbezogenen (z.B. Adress-)Daten über ihre Vertragspartner, die Eltern. Verantwortlich für diese Daten sind damit die Jugendämter. Die Senatsverwaltung stellt lediglich im Wege der sog. Auftragsdatenverarbeitung das IT-Fachverfahren[160] zur Verarbeitung der Vertragsdaten zur Verfügung. Eine Nutzung dieser Daten durch die Senatsverwaltung (z.B. zur Versendung von Werbebriefen) ist dabei nicht vorgesehen und kann auch nicht auf die Vorschriften des Kindertagesförderungsgesetzes und der dazugehörenden Rechtsverordnung gestützt werden. Wir haben die Nutzung der Vertragsdaten zur Versendung des Elternbriefs mangels Rechtsgrundlage als erheblichen Verstoß gegen daten-

160 Integrierte Software Berliner Jugendhilfe – ISBJ

schutzrechtliche Bestimmungen gegenüber dem Regierenden Bürgermeister und dem Senator für Bildung, Wissenschaft und Forschung beanstandet. Dieser teilte uns mit, unsere Hinweise in seiner Behörde zur Kenntnis und zur Beachtung zu geben. Wir haben die Thematik auf Fachebene mit der Senatsverwaltung erörtert. Positiv hervorzuheben ist, dass die im Entwurf vorliegende Änderungsverordnung zur Kindertagesförderungsverordnung nunmehr eine Regelung vorsieht, nach der die bezirklichen Jugendämter auf Anregung der Senatsverwaltung berlinweite Informationen im Bereich der Kindertagesförderung in eigener Zuständigkeit übermitteln können.

Zukünftig wird gewährleistet, dass allein die Jugendämter als verantwortliche Stellen auf die Daten der Eltern zugreifen und auf diesem Weg auch berlinweite Informationen versenden können.

7.1.2. Weitergabe von Informationen über säumige Kita-Eltern

Aus der Praxis

Ein Jugendamt bat uns um Auskunft, ob es datenschutzrechtlich zulässig ist, wenn die Leitung einer Kindertageseinrichtung (Kita) Eltern gezielt auf Rückstände bei der Zahlung der monatlichen Kita-Beiträge anspricht. Bei Eltern, die sich in einem erheblichen Zahlungsrückstand mit den Beiträgen befinden, bestehe die Gefahr, dass sich Schulden anhäuften und in der Folge die Kündigung des Kita-Platzes drohe. Es liege sowohl im Interesse des Kindes und seiner Eltern als auch im Interesse der Kita und des Trägers, mit den betroffenen Familien zeitnah eine Klärung herbeizuführen. Schriftliche Mahnungen durch die Verwaltung des Trägers führten in der Praxis häufig nicht zum Erfolg. Da die pädagogische Leitung der Kita einen persönlichen Kontakt zu den Eltern habe, führe der Weg über die Kita-Leitung häufiger zu einer Problemlösung.

Aus Datenschutzsicht stellt sich das Problem, dass zumindest bei großen Trägern die Verwaltung und der pädagogische Bereich voneinander getrennt sind. Grundsätzlich handelt es sich um funktional getrennte Einheiten, die verschiedene Aufgaben wahrnehmen und damit als unterschiedliche Daten verarbei-

tende Stellen anzusehen sind. Teilt die Verwaltung der pädagogischen Leitung mit, dass Beitragsschulden – für deren Einziehung die Verwaltung zuständig ist – bestehen, werden personenbezogene Daten übermittelt, was im Einklang mit den datenschutzrechtlichen Vorschriften erfolgen muss. Die Übermittlung muss insbesondere erforderlich für die Erfüllung des pädagogischen Auftrages sein. Im konkreten Fall sind wir zu dem Ergebnis gekommen, dass die Ansprache der Eltern durch die Kita-Leitung, die die Familie persönlich kennt, zur Vermeidung einer Kündigung vom pädagogischen Auftrag erfasst ist und im Interesse des Kindes liegt. Wir halten die Mitteilung der Tatsache, dass eine Kündigung des Betreuungsvertrages droht, für datenschutzrechtlich zulässig. Zu beachten ist hierbei allerdings, dass dies nicht diejenigen Fallkonstellationen betrifft, in denen geringfügige Beitragsrückstände bestehen, sondern jene, in denen tatsächlich eine Kündigung des Platzes droht, die es im Interesse des Kindes abzuwenden gilt. Hinsichtlich der Mitteilung der Höhe der bestehenden Rückstände bedarf es allerdings einer konkreten Prüfung in jedem Einzelfall.

Wir gehen davon aus, dass das Verfahren geeignet ist, durch eine persönliche Kontaktaufnahme der Kita-Leitung zu den Eltern einen Weg finden zu können, um eine Kündigung des Kita-Platzes zu verhindern. Dies ist im Interesse des Kindes wichtig. Wir haben empfohlen, das Verfahren im Falle verspäteter Zahlungen gegenüber den Eltern, z. B. durch eine entsprechende Formulierung im Betreuungsvertrag, transparent zu machen.

7.1.3 Handreichung zur Datenübermittlung bei Kinder- und Jugenddelinquenz fertig

Im Bereich der Kinder- und Jugenddelinquenz werfen die für eine Steigerung der Effektivität notwendigen zügigen Informationsflüsse zwischen den verschiedenen beteiligten Stellen Fragen nach der datenschutzrechtlichen Zulässigkeit auf. Unser Anliegen ist es, insbesondere den Beschäftigten in der Jugendhilfe bestehende Rechtsunsicherheiten zu nehmen und ihnen für verschiedene Fallkonstellationen ein Gerüst an die Hand zu geben, um diese datenschutzrechtlich einordnen zu können.

2010 hatten wir über unsere Mitarbeit an dem Entwurf einer „Handreichung zur Datenübermittlung im Bereich Kinder- und Jugenddelinquenz“ berichtet, der im Rahmen der unter der Federführung der Senatsverwaltung für Bildung, Wissenschaft und Forschung tagenden „Ressortübergreifenden Arbeitsgruppe Kinder- und Jugenddelinquenz“ erarbeitet worden ist.[161] Die Handreichung wurde nunmehr fertiggestellt und steht den Berliner Jugendämter, der Polizei, der Staatsanwaltschaft, der Jugendgerichte, der Schulen, der Bewährungshilfe, des Strafvollzugs sowie der Freien Träger der Jugendhilfe zur Verfügung.

Die „Ressortübergreifende Arbeitsgruppe Kinder- und Jugenddelinquenz“ hat sich nun mit der Zusammenarbeit im Bereich der Kinder- und Jugenddelinquenz befasst. Wir haben uns intensiv beteiligt. Hintergrund war die in Berlin und in anderen Bundesländern geführte Diskussion über die Durchführung von ressortübergreifenden **Fallkonferenzen**. Dies sind regelmäßig tagende Gremien, die mit Vertreterinnen und Vertretern mehrerer Disziplinen (wie Polizei, Schule, Jugendhilfe) besetzt sind und sich einzelfallbezogen über kindliche bzw. jugendliche Schwellen- und Intensivtäterinnen und -täter austauschen. Soweit in Berlin Fallkonferenzen durchgeführt wurden, war eine sehr uneinheitliche Praxis festzustellen. Daraus ergab sich die Notwendigkeit, einheitliche und verbindliche Verfahrensweisen festzulegen. Zunächst war festzustellen, ob derartige Konferenzen wirklich zielführend sein können und welche Arbeitsabläufe dazu geführt haben, dass die bisherige Zusammenarbeit als nicht ausreichend angesehen wird. Hierbei stellte sich heraus, dass es bei den Problemen in der Zusammenarbeit nur teilweise um einen konkreten Datenaustausch geht. Im Vordergrund steht vielmehr das für die Zusammenarbeit erforderliche gegenseitige Vertrauen in die Professionalität des jeweils anderen. Es wurden Maßnahmen zur Beschleunigung von Verfahrensabläufen und zur Verbesserung der Kooperationsstrukturen festgelegt. Im Ergebnis der Diskussion bestand Einigkeit darüber, in Berlin zum gegenwärtigen Zeitpunkt Abstand von Fallkonferenzen zu nehmen. Diese Ergebnisse der Arbeitsgruppe wurden in einem Rundschreiben der Senatsverwaltung für Bildung, Wissenschaft und Forschung zusammengefasst.[162]

161 JB 2010, 8.1.5

162 Jugend-Rundschreiben Nummer 5/2011 zur Verbesserung der interdisziplinären ressortübergreifenden Zusammenarbeit im Umgang mit Mehrfach- und Intensivtätern (Klärung der Notwendigkeit von Fallkonferenzen im Land Berlin) vom 20. September 2011, ABl. S. 2737

Ein ressortübergreifender Austausch personenbezogener Daten im Rahmen von Fallkonferenzen ist vom Gesetzgeber nicht vorgesehen und berührt in besonderer Weise datenschutzrechtliche Grundprinzipien. Wir gehen davon aus, dass sich durch Verbesserung der Verfahrensabläufe und Kooperationsstrukturen die in der Praxis festgestellten Defizite in der Zusammenarbeit in Zukunft vermeiden lassen. Häufig wird der im Rahmen der geltenden datenschutzrechtlichen Bestimmungen im Einzelfall zulässige Austausch personenbezogener Daten im bilateralen Verhältnis für die Klärung des Einzelfalls ausreichend sein.

7.1.4 Gerichtsvollzieher arbeiten nicht für das Jugendamt

Im Juni wurden wir durch eine Pressemitteilung der Senatsverwaltung für Bildung, Wissenschaft und Forschung auf einen Handlungsleitfaden zur Zusammenarbeit zwischen Gerichtsvollziehern und bezirklichem Jugendamt im Kinderschutz aufmerksam. Die Senatsverwaltung kündigte darin an, Gerichtsvollzieher würden in Berlin künftig eine stärkere Rolle im vorbeugenden Kinderschutz spielen. In Ausübung ihres Amtes sollten sie darauf achten, ob es in von ihnen aufgesuchten Wohnungen Anzeichen für eine Kindeswohlgefährdung gebe, und daraufhin die Jugendämter informieren. Hierfür wurde ein Meldebogen für die Gerichtsvollzieher entwickelt, mit dem sie ihre Beobachtungen (z.B. Anhaltspunkte für Desinteresse am Schulbesuch der oder des Minderjährigen, Entwicklungsverzögerungen von Minderjährigen) dem Jugendamt mitteilen sollten.

Das Anliegen, Gerichtsvollziehern, die bei ihrer Aufgabenerfüllung Anzeichen einer Kindeswohlgefährdung wahrnehmen, eine Hilfestellung an die Hand zu geben, an welche Institution sie sich wenden können, und ihnen Kontaktdaten der Jugendämter zur Verfügung zu stellen, ist nachvollziehbar und datenschutzrechtlich nicht zu beanstanden. Allerdings entstand durch den Handlungsleitfaden der Eindruck, es bestehe eine Verpflichtung für die Gerichtsvollzieher zur Meldung gegenüber dem Jugendamt. Der im Text enthaltene Hinweis, Gerichtsvollzieher erhielten im Rahmen ihrer Aufgabenerfüllung Zugang zu Wohnungen und damit Einblick in die Intimsphäre der Menschen bzw.

Familien, erweckte den Anschein, Gerichtsvollzieher sollten als „verlängerter Arm“ des Jugendamtes tätig werden und hätten die Aufgabe, im Rahmen ihres – ganz anderen Zwecken dienenden – Hausbesuches Kindeswohlgefährdungen aufzudecken. Da das Vorliegen der im Meldebogen enthaltenen Kriterien für eine Kindeswohlgefährdung selbst von Sozialarbeiterinnen und -arbeitern im Einzelfall schwer beurteilt werden kann, ist es nicht sinnvoll, die Gerichtsvollzieher mit derartigen Einschätzungen zu überfordern und diese anzuhalten, Daten über die Familien zu erheben, um sie dem Jugendamt mitzuteilen.

Es geht uns nicht darum, Gerichtsvollziehern, die eindeutige Anzeichen von Kindeswohlgefährdungen wahrnehmen, die Möglichkeit zu nehmen, tätig zu werden, d. h. insbesondere die Polizei zu informieren, damit diese geeignete Maßnahmen zur Abwendung der Gefahr treffen und ggf. ihrerseits das Jugendamt informieren kann. Allerdings entstand der Eindruck, die Gerichtsvollzieher hätten die Aufgabe, nach allgemeinen Anhaltspunkten für eine Kindeswohlgefährdung zu suchen. Dies ist mit den gesetzlichen Aufgaben der Gerichtsvollzieher unvereinbar.

Als Reaktion auf unsere sowie die von der Senatsverwaltung für Justiz vorgebrachte Kritik entschied die Senatsverwaltung für Bildung, Wissenschaft und Forschung, dass der Handlungsleitfaden nicht weiter verwendet wird.

Mit dem Verzicht auf die Verwendung des Handlungsleitfadens in der Praxis werden Missverständnisse und die Gefahr unnötiger und damit unzulässiger Datenübermittlungen an die Jugendämter vermieden. Wünschenswert wäre eine frühzeitige Beteiligung unserer Behörde gewesen.

7.1.5 Buchungssoftware der Berliner Unterbringungsleitstelle

Zu Beginn des Jahres erhielten wir aus dem Kreis der behördlichen Datenschutzbeauftragten einen Hinweis, dass das Landesamt für Gesundheit und Soziales (LaGeSo) die Buchungssoftware der Berliner Unterbringungsleitstelle (BUL) modernisiert.

Mithilfe dieses Verfahrens wird die Belegung von Plätzen in den Berliner Obdachlosenheimen zentral durch das LaGeSo organisiert. Das bisherige Verfahren bestand im Wesentlichen aus einer zentralen Datenbank, die eine Übersicht über die vorhandenen Plätze in den diversen Berliner Obdachlosenheimen enthielt und die Organisation der Vergabe dieser Plätze erlaubte. Die Kommunikation mit den bezirklichen Anlaufstellen erfolgte telefonisch. Eine Verarbeitung personenbezogener Daten fand im alten Verfahren nicht statt.

Auf Wunsch der Bezirke erfolgte 2010 eine Umstellung des Verfahrens auf eine Client-Server-Architektur, in der auch personenbezogene Daten verarbeitet werden. Die Modernisierung des Verfahrens sollte die Möglichkeit der Erfassung und Bearbeitung der Daten durch die bezirklichen Anlaufstellen eröffnen. Als Grundlage dienten eine Verwaltungsvereinbarung von 2005 sowie statistische Anforderungen der Senatsverwaltung für Integration, Arbeit und Soziales. Unsere Beteiligung nach § 24 Abs. 3 Satz 3 BlnDSG wurde versäumt.

In diesem Jahr sollte eine webbasierte Lösung geschaffen werden. Die uns auf Nachfrage übersandten Unterlagen beinhalteten u.a. ein Sicherheitskonzept, das im Wesentlichen für das ursprüngliche Verfahren vor 2010 konzipiert wurde und nur marginale Anpassungen an den derzeitigen Zustand aufwies. Durch die Umstellung von einem lokalen auf ein berlinweites Verfahren und wegen der erstmaligen Verarbeitung personenbezogener Daten hätte auch das Sicherheitskonzept einer entsprechenden Revision unterzogen werden müssen.

Rechtsgrundlagen, die die Verarbeitung der personenbezogenen Daten durch die Buchungssoftware legitimieren würden, konnten uns nicht benannt werden. Diese sind aber für einen rechtmäßigen Einsatz des Verfahrens erforderlich. Eine hilfsweise Einwilligung der Betroffenen in die Verarbeitung ihrer Daten

würde aufgrund der Notlage, in der sich Obdachlose in der Regel befinden, nicht auf einer freien Entscheidung beruhen und daher wegen § 6 Abs. 5 Satz 1 BlnDSG unwirksam sein.

Für das Verfahren BUL des Landesamtes für Gesundheit und Soziales ist weder eine Rechtsgrundlage erkennbar, noch liegt ein Sicherheitskonzept vor, das vor einer Entscheidung über den Einsatz oder einer wesentlichen Veränderung der automatisierten Verarbeitung vorliegen und mit dem Einsatz umgesetzt sein muss.

7.2 Gesundheitswesen

7.2.1 Orientierungshilfe Krankenhausinformationssysteme

Im Frühjahr beschlossen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der Düsseldorfer Kreis[163] und die Datenschutzbeauftragten der katholischen und evangelischen Kirchen eine Orientierungshilfe für die Datenverarbeitung in Krankenhäusern.

Nach zwei Jahren intensiver Arbeit und Abstimmung mit Experten aus der Wissenschaft, mit Herstellern und Krankenhäusern wurde im Februar durch die Unterarbeitsgruppe Krankenhausinformationssysteme (UAG KIS) unter unserer Federführung eine Orientierungshilfe fertiggestellt, die für die kommenden Jahre die Prüfpraxis der Kontrollbehörden in den Krankenhäusern bestimmen wird. Wir hoffen, dass von dieser Orientierungshilfe ein wesentlicher Impuls für die Hebung des Datenschutzniveaus ausgehen wird. Sie nimmt nicht nur die Praxis der Krankenhäuser als Betreiber der Informationssysteme ins Visier, sondern wendet sich auch an die Hersteller dieser Systeme und nimmt sie in die Pflicht, ihre Produkte so zu gestalten, dass ein effektiver Datenschutz im Krankenhaus möglich wird.

163 Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Die Orientierungshilfe rief ein vielfaches, differenziertes Echo hervor. Sie wurde mehrfach publizistisch aufgegriffen. Vereinigungen von Anwendern verbreiteter Informationssysteme bildeten Arbeitsgruppen, die sich der Ausgestaltung des Datenschutzes bei dem Betrieb dieser Systeme widmen. Auch der neu geformte Herstellerverband bvitg (Bundesverband Gesundheits-IT) koordinierte die Anstrengungen seiner Mitglieder in diesem Bereich, die bereits zu ersten Erweiterungen und neuen Features der Produkte geführt haben. Die Reaktionen der Krankenhäuser wurden von der Deutschen Krankenhausgesellschaft (DKG) gebündelt. Die UAG KIS führte intensive Gespräche mit der DKG mit dem Ziel, ein einheitliches Verständnis der Anforderungen zu erreichen. Die Protokolle dieser Gespräche stehen der interessierten Öffentlichkeit zur Verfügung. Ihnen ist der sehr weite Grad der Übereinstimmung zu entnehmen, der bei den Gesprächen erzielt worden ist.

Hier wie auch in einer berlinweiten Informationsveranstaltung, die wir zu dem Themenkomplex organisierten und zu der wir Vertreter aller Berliner Krankenhäuser einluden[164], haben wir stets betont: Datenschutz im Krankenhaus ist ein komplexer Prozess, dessen Zielpunkt einer vollständigen Gesetzeskonformität sich nicht über Nacht erreichen lässt. Er bedarf in jedem einzelnen Krankenhaus zielorientierter Planung, ausreichender personeller und sachlicher Ressourcen und eines klaren Zeitplans für die Umsetzung der einzelnen Maßnahmen.

In unserer eigenen Prüfpraxis legten wir die Orientierungshilfe der Beurteilung der Datenschutzkonzepte für die elektronische Patientenakte zweier großer Berliner Krankenhäuser zugrunde. Wir begrüßen, dass beide Institutionen Anstrengungen unternommen haben, den ehemals über die Maßen freizügigen Zugriffsmöglichkeiten Grenzen zu setzen. Mit der Umsetzung der Konzepte werden sie der Gewährleistung näher kommen, dass auf die sensiblen Informationen über die Gesundheit der Patientinnen und Patienten nur soweit zugegriffen wird, wie das für die Behandlung, ihre Abrechnung und die Verwaltung der Prozesse im Krankenhaus erforderlich ist. Eine für den Laien erstaunliche Zahl von Beschäftigten in Krankenhäusern hat Zugriff auf Patientendaten. Dies ist durch die Arbeitsteilung im Krankenhaus bedingt. Leider bleibt auch nach

164 Siehe 15.4

Umsetzung der geprüften Konzepte die Zahl der von vornherein Zugriffsberechtigten noch um ein Vielfaches zu hoch.

Das Rezept hiergegen liegt in einer Klärung und Umgrenzung der Zuständigkeiten sowie einer Dynamisierung der Zugriffsrechte: Erst wenn eine diagnostische Leistung angefordert wird, Kolleginnen und Kollegen einer anderen Fachabteilung um ihren konsiliarischen Rat gefragt werden oder eine wechselnden Stationen zugeordnete Pflegekraft den Dienst in einer neuen Station aufnimmt, dürfen die jeweils erforderlichen Rechte in Kraft treten.

Die Berliner Krankenhäuser sind aufgefordert, die Orientierungshilfe Krankenhausinformationssysteme zu nutzen, um ihre Datenverarbeitung einer Revision zu unterziehen und Aktionspläne zu entwickeln, die in einem überschaubaren Zeitraum zu einem rechtskonformen Betrieb ihrer Informationssysteme führen.

7.2.2 Gemeinsamer Betrieb von Informationssystemen durch verschiedene medizinische Einrichtungen

Aus der Praxis

Eine Reihe von Berliner Krankenhäusern kooperiert eng mit ambulanten Leistungserbringern, insbesondere Medizinischen Versorgungszentren in eigener rechtlicher Trägerschaft. Bei einer Prüfung fanden wir eine unzulässige Verschränkung der Datenverarbeitung von Krankenhaus und ambulanter Einrichtung. Auch waren die rechtlichen Verantwortlichkeiten nicht hinreichend geklärt.

Nach ihrer Entlassung werden Patientinnen und Patienten eines Krankenhauses vielfach von ambulanten Einrichtungen betreut, die eng mit dem Krankenhaus kooperieren. Einzelne Ärztinnen und Ärzte und anderes Personal arbeiten in beiden Einrichtungen. Davon profitieren die Kranken. Die Einrichtungen liegen sich räumlich sehr nahe. Es erscheint natürlich, dass auch IT-Ressourcen gemeinsam genutzt werden: Das Krankenhaus stellt der ambulanten Einrichtung IT-Geräte und die Dienste seines kompetenten IT-Personals zur Verfügung. In dem von uns geprüften Fall wurde zudem ein einheitliches Infor-

mationssystem genutzt und Datenzugriffe über die Grenzen der Institutionen hinaus ermöglicht. Die Gestaltung einer derartigen, durchaus sowohl medizinisch wie wirtschaftlich wünschenswerten Zusammenarbeit muss zweierlei gewährleisten: Zum einen die Transparenz für die Kranken und die Beachtung ihres Willens bezüglich der mit einer solchen Verquickung verbundenen Offenbarung ihrer Daten an die jeweils andere Seite, zum anderen eine klare gesetzeskonforme vertragliche Regelung der Verantwortlichkeiten.

In der geprüften Situation hatten die Patientinnen und Patienten dagegen keine Wahl: Wer sich in der ambulanten Einrichtung behandeln ließ, dessen Daten fanden sich unweigerlich auch im Krankenhaus wieder. Die vertraglichen Vereinbarungen waren rudimentär. Übermittlungen von einer Stelle zur anderen ließen sich nicht nachvollziehen. Der Gesetzgeber hat es bisher unterlassen, eine Abwägung der Interessen der Kranken an der Verschwiegenheit ihrer Ärztinnen und Ärzte und dem der Allgemeinheit an einer effizienten medizinischen Leistungserbringung dahingehend vorzunehmen, dass dem ärztlichen Personal die Verarbeitung von Behandlungsdaten im Auftrag durch Dritte generell gestattet ist.

Damit muss die freie Wahl bei den Patientinnen und Patienten bleiben. Frei ist die Wahl jedoch nur, wenn der ambulante Leistungserbringer sie nicht vor die Wahl stellt, entweder der Speicherung ihrer Daten im Krankenhaus zuzustimmen oder auf die angebotene spezialisierte Behandlung zu verzichten, die zudem teilweise von Ärztinnen und Ärzten erbracht wird, die sie bereits aus dem Krankenhaus kennen. Nur wenige werden etwas gegen die aushäusige Speicherung einzuwenden haben. Es ist zumutbar, für diese Wenigen ein alternatives Verfahren der ambulanten Einrichtung bereitzuhalten, das für die geringen zu erwartenden Fallzahlen auch nur eine geringe Kapazität zu haben braucht.

Für die Mehrheit der Fälle kommt die im Krankenhaus betriebene und administrierte Software zum Einsatz. Die Daten der ambulanten Einrichtung müssen hierbei als solche gekennzeichnet bleiben, die Zugriffsrechte auf Weisung der Leitung der ambulanten Einrichtung erteilt und separat von den Rechten der Beschäftigten des Krankenhauses verwaltet werden. Die Anforderungen betreffen nicht nur den Umgang mit den aktuell im Gebrauch befindlichen Daten, sondern auch Archivdaten, die Datensicherungen, Sperr- und

– aufgrund der unterschiedlichen gesetzlichen Aufbewahrungspflichten – auch Löschvorgänge. Voraussetzung der technischen Umsetzbarkeit ist die sog. Mandantenfähigkeit des verwendeten Informationssystems. Die gemeinsame Datenhaltung in einem Mehrmandantensystem vereinfacht auch den Austausch von z.B. Befunden und Arztbriefen. Doch auch hier gilt das Gleiche wie für jeden Austausch zwischen verschiedenen Ärztinnen und Ärzten, die ein und dieselbe Person behandeln: Er ist nur mit deren Wissen und Wollen zulässig. Bei einem kontinuierlichen Behandlungsgeschehen, in dem die Patientin oder der Patient zwischen den Einrichtungen wechselt, ist von dem Einverständnis der Kranken auszugehen. Ein Widerspruch ist jedoch zu beachten. Für komplexere und schwerer zu überschauende Situationen etwa der Integrierten Versorgung oder eines anderweitigen Versorgungsmanagements durch das Krankenhaus schreibt der Gesetzgeber ausdrückliche Einwilligungen vor.

Aufgrund unseres Einwirkens fassten im vorliegenden Fall die beteiligten Stellen ihre vertraglichen Beziehungen neu und beseitigten nicht erforderliche Zugriffsmöglichkeiten. Die gesetzlich geforderte Gewährleistung der Nachvollziehbarkeit der Datenflüsse und die Gestaltung des angesprochenen alternativen Verfahrens für die Verwaltung von Patientenakten stehen noch aus.

Eine gemeinsame Nutzung von Informationssystemen durch Krankenhäuser und rechtlich selbständige ambulante Einrichtungen ist nur möglich, wenn sie für die Patientinnen und Patienten transparent gehandhabt wird, ihre Rechte gewahrt bleiben und die Verantwortlichkeiten vertraglich eindeutig geregelt werden.

7.2.3 Pseudonymisierte Datenübermittlung an das Tumorzentrum Berlin

Ein Krankenhaus wollte wissen, unter welchen Bedingungen Krankenhäuser rechtmäßig Daten an das Tumorzentrum Berlin übermitteln können.

Das Tumorzentrum Berlin e. V. (TZB) wertet Daten über die Behandlung von Menschen aus, die an einem Krebsleiden erkrankt sind, um die Qualität der

onkologischen Behandlung in Berlin zu erhöhen. Es erhält die Daten von den fünf regionalen Tumorzentren, die an Berliner Krankenhäusern eingerichtet wurden.

Bis zur Novellierung des Berliner Landeskrankenhausgesetzes[165] konnte sich eine solche Übermittlung nur auf die Einwilligung der Patienten stützen. Dem TZB erschien es wünschenswert, die Übermittlung auch dann bereits aufzunehmen, wenn den Patientinnen und Patienten die Krebsdiagnose noch gar nicht bekannt war. Daher wurden unterschiedslos alle gefragt, ob sie für den Fall einer entsprechenden Erkrankung schon vorab ihr Einverständnis hierzu erklären wollen. Wer jedoch keine klare Vorstellung über das Wie, Wann und Wozu einer Datenverarbeitung hat, kann ihr nicht wirksam zustimmen.

Seit Oktober ist es den Krankenhäusern erlaubt, an eine ärztlich geleitete Stelle Daten zu übermitteln, wenn hierdurch Erkenntnisse gewonnen werden, die helfen, die Qualität der Behandlungsvorgänge in dem Krankenhaus zu sichern oder zu heben. Es ist möglich, die Qualität einer Behandlung einzuschätzen, ohne dass Angaben über Namen und Identität vorliegen. Dies gilt auch hier. Das Gesetz fordert in diesem Fall, dass statt der Namen und anderen Angaben über die Identität der behandelten Person nur ein Pseudonym übermittelt wird.

Krebspatienten werden oft in verschiedenen Häusern behandelt. Daher liegen die Angaben über ihre Behandlung auch nur verteilt vor. Soll beurteilt werden, ob die Behandlung den wissenschaftlichen Erkenntnissen und bestehenden Leitlinien genügt, wird eine Zusammenschau auf die gesamte Behandlung benötigt. Es ist daher wichtig, dass Daten zweier verschiedener Einrichtungen über dieselbe Person auch dasselbe Pseudonym erhalten, damit dem TZB eine Zusammenführung ermöglicht wird.

Die Zuordnung von Namen zu Pseudonymen wird am einfachsten garantiert, wenn sie in einer Hand liegt. Die Aufgabe kann von einer Vertrauensstelle übernommen werden, die im Auftrag für alle beteiligten Krankenhäuser tätig wird. Medizinische Angaben über die Patientinnen und Patienten benötigt sie für ihre Aufgabe nicht. Doch bereits das Wissen darüber, wer in Berlin an Krebs erkrankt ist, ist schützenswert. Daher darf die Vertrauensstelle entsprechend

165 Siehe 2.2.2

den Vorgaben des Landeskrankenhausgesetzes zur Auftragsdatenverarbeitung nur bei einem Krankenhaus eingerichtet werden. Wie jede Verarbeitung von Daten im Auftrag bedarf sie einer vertraglichen Grundlage. Wir haben eines der regionalen Tumorzentren, bei dem eine Vertrauensstelle eingerichtet werden soll, darin unterstützt, einen Mustervertrag zu erarbeiten. Wie im oben beschriebenen Fall ist es erforderlich, auch die technischen Maßnahmen zu berücksichtigen, die zum Schutz der Daten bei ihrem Transport von und zu der Vertrauensstelle sowie bei ihrer Verarbeitung dort zu treffen sind. Die Verarbeitung muss auf einem für den hohen Schutzbedarf besonders gesicherten Server erfolgen, auf den nur ein eng begrenzter Personenkreis Zugriff nehmen kann.

Das Tumorzentrum Berlin darf zur Sicherung der Qualität der Behandlung Daten von krebskranken Patientinnen und Patienten von Berliner Krankenhäusern erhalten und verarbeiten. Die Daten sind vorher von einer Vertrauensstelle zu pseudonymisieren.

7.2.4 Der gefährliche USB-Stick

Ein Petent übergab uns einen USB-Stick, auf dem eine Zahnarztpraxis sein Röntgenbild gespeichert hatte. Nach der Speicherung erwies sich, dass das Gerät mit einem Virus infiziert war.

Patienten haben das Recht, von ihren Ärztinnen und Ärzten Kopien von elektronisch vorliegenden Röntgenbildern zu erhalten. Die betreffende Zahnarztpraxis kam dieser Verpflichtung nach, indem sie die Bilder auf Medien speicherte, die ihr von den Patienten übergeben wurden. Ist eines der übergebenen Medien mit einem Virus infiziert, so kann dieser unter bestimmten Umständen auch auf den Rechner übertragen werden, mit dem es verbunden wird. Darin liegen schwer kontrollierbare Risiken für die Patientendaten, die auf diesem Rechner gespeichert oder mit ihm verarbeitet werden. Außerdem können, wie höchstwahrscheinlich im vorliegenden Fall geschehen, auch die Medien anderer Patienten infiziert werden, sodass der Virus weiter verbreitet wird.

Wir haben die Praxis darauf hingewiesen, dass das gewählte Vorgehen nicht zulässig ist und eine Gefährdung von Patientendaten bewirkt. Auf unseren Vorschlag benutzt die Praxis nunmehr fabrikneue, einmal beschreibbare CDs zur Übergabe der Bilddaten an die Patienten.

Zur Speicherung von Röntgenbildern und anderen Patientendaten außerhalb des Praxissystems dürfen nur eigene, fabrikneue oder gut kontrollierte Speichermedien verwendet werden. Der Anschluss fremder USB-Geräte ist auszuschließen.

7.2.5 Einsichtsrecht von Patienten gestärkt

Wir sind darauf aufmerksam gemacht worden, dass die Berufsordnung der Ärztekammer Berlin das Einsichtsrecht von Patientinnen und Patienten in ärztliche Dokumentation unangemessen einschränkt. Die Berufsordnung sieht vor, dass subjektive Eindrücke oder Wahrnehmungen, die sich die Ärztin bzw. der Arzt über die Patientinnen und Patienten in der Krankenakte notiert hat, vom Einsichtsrecht der Betroffenen ausgenommen sind.

Grundsätzlich haben Patientinnen und Patienten das Recht, Einblick in alle über sie gespeicherten Daten, insbesondere in die Krankenunterlagen, zu nehmen. Nach der Rechtsprechung des Bundesverfassungsgerichts ist es unzulässig, bestimmte Teile der Patientendokumentation den Betroffenen pauschal vorzuenthalten.[166] Vielmehr muss im Einzelfall eine Abwägung zwischen dem informationellen Selbstbestimmungsrecht der Betroffenen auf der einen und legitimen Interessen am Ausschluss der Akteneinsicht auf der anderen Seite vorgenommen werden. Solche Interessen können z.B. betroffen sein, wenn die Patientenakte personenbezogene Daten Dritter enthält oder wenn konkrete Anhaltspunkte bestehen, dass die Patientin oder der Patient aufgrund der Akteneinsicht sich selbst oder andere gefährdet. Solche Fälle können z.B. im Bereich der Psychiatrie auftreten, sie bilden aber auch dort die absolute

166 BVerfG, 1 BvR 1130/98, NJW 1999, S. 1777

Ausnahme. Im Regelfall hat die Ärztin bzw. der Arzt vollständige Akteneinsicht zu gewähren.

Die Gründe für die ursprüngliche Beschränkung des Einsichtsrechts sind historisch zu erklären. Früher ging man davon aus, dass die Patientendokumentation einzig den Ärztinnen und Ärzten diene und den Patientinnen und Patienten nur beschränkte Rechte im Zusammenhang mit ihrer Behandlung zustehen. Dieses Verständnis hat sich jedoch im Laufe der Zeit gewandelt. Heute geht man weniger von „vertrauenden Kranken" als von mündigen und selbstbewussten Patientinnen und Patienten aus, die in der Lage sind, selbst darüber zu bestimmen, was bei einer ärztlichen Behandlung mit ihnen geschieht. Dazu ist es erforderlich, dass sie sich informieren können und dabei auch Einsicht in die über sie gespeicherten Angaben nehmen können. Schließlich handelt es sich bei Gesundheitsdaten um besonders sensitive Informationen, die häufig die engste Privat- oder die Intimsphäre betreffen. Daher darf nur in eng begrenzten Ausnahmefällen die Einsicht verweigert werden, wenn dafür triftige Gründe bestehen.

Wir haben die Ärztekammer Berlin darauf aufmerksam gemacht, dass die Berufsordnung nicht der geltenden Rechtslage entspricht. Die Kammer hat zugesagt, die Berufsordnung entsprechend zu ändern, sodass die Beschränkung der Akteneinsicht auf nur objektive Inhalte beseitigt würde. Bis zu einer solchen Änderung würden die Ärztinnen und Ärzte aber bereits im Sinne der aktuellen Rechtsprechung beraten. Auch das Landeskrankenhausgesetz enthielt bisher eine Beschränkung auf objektive Inhalte, die nunmehr entfallen ist.[167]

Patientinnen und Patienten haben ein Recht auf umfassende Einsicht der Krankenunterlagen. Es ist unzulässig, bestimmte Teile der Patientenakte den Betroffenen pauschal vorzuenthalten. Abweichungen von diesem Grundsatz sind nur ausnahmsweise zu Gunsten höherer Schutzgüter möglich, wenn z. B. im Einzelfall konkrete Anhaltspunkte dafür bestehen, dass sich die Betroffenen bei Kenntnis des Akteninhalts selbst oder Dritte gefährden.

167 Siehe 2.2.2

7.2.6 Datenübermittlung aus berufsrechtlichem Verfahren der Ärztekammer Berlin

Ein Arzt beschwerte sich darüber, dass die Ärztekammer Berlin Einzelheiten aus einem berufsrechtlichen Untersuchungsverfahren an die Kassenärztliche Vereinigung (KV) Berlin übermittelt habe.

Die Ärztekammer führt ein Berufsverzeichnis, in das u.a. berufsgerichtliche Maßnahmen sowie Daten zur Erfüllung der Berufspflichten aufzunehmen sind. Aus diesem Berufsverzeichnis dürfen Auskünfte an Gerichte, Behörden und Körperschaften des öffentlichen Rechts erteilt werden. Im vorliegenden Fall übermittelte die Ärztekammer im Rahmen eines laufenden Ermittlungsverfahrens konkrete Verdachtsmomente hinsichtlich eines zu prüfenden Berufsverstoßes an die KV. Die Ärztekammer ging davon aus, dass die Übermittlung von Daten aus einem laufenden berufsrechtlichen Ermittlungsverfahren ebenfalls von der im Kammergesetz vorgesehenen Befugnis zur Übermittlung von Inhalten des Berufsverzeichnisses umfasst sei.

Eine Datenübermittlung auch zwischen öffentlichen Stellen ist nur zulässig, wenn sie mit Einverständnis der Betroffenen oder auf Grundlage einer Rechtsvorschrift erfolgt.[168] Hier lag weder das Einverständnis des Petenten noch eine einschlägige Rechtsgrundlage vor.

Eine Auslegung, wonach auch bereits erhobene Daten aus einem laufenden Ermittlungsverfahren als Teil des Berufsverzeichnisses an Dritte übermittelt werden dürfen, widerspricht der Systematik des Berliner Kammergesetzes. In den Vorschriften zu den berufsgerichtlichen Maßnahmen ist ausdrücklich geregelt, dass diese erst nach Eintritt der Rechtskraft, mithin einen Monat nach dem Urteil, in das Berufsverzeichnis eingetragen werden und dort nach Ablauf von fünf Jahren gelöscht werden müssen. Eine entsprechende Regelung besteht für gegenüber Kammermitgliedern ausgesprochene Rügen. Bei beiden Verfahren handelt es sich um bereits abgeschlossene Verfahren, bei denen jeweils eine Verletzung der Berufspflicht positiv festgestellt worden ist. Zum Zeitpunkt

168 § 6 BlnDSG

eines laufenden berufsrechtlichen Untersuchungsverfahrens muss hingegen noch geprüft werden, inwieweit sich der Verdacht einer Berufspflichtverletzung überhaupt erhärtet. Die Regelungen zur Aufnahme in das Berufsverzeichnis hinsichtlich einer berufsgerichtlichen Maßnahme bzw. Rüge wären obsolet, wenn bereits alle im Untersuchungsverfahren erhobenen Daten Teil des Berufsverzeichnisses wären und insoweit an andere öffentliche Stellen übermittelt werden dürften.

Dieses Ergebnis ist auch sachgerecht. Im Hinblick auf das Persönlichkeitsrecht der Betroffenen und die Unschuldsvermutung ist es nicht vertretbar, Dritten Details und bloße Verdachtsmomente aus laufenden Untersuchungsverfahren mitzuteilen. Eine Ausnahme, wonach bei bestehender akuter Gefahr für das Patientenwohl eine Datenübermittlung zulässig wäre, lag ebenfalls nicht vor.

Wir haben die Datenübermittlung an die Kassenärztliche Vereinigung gegenüber der Ärztekammer beanstandet. Diese teilte uns daraufhin mit, dass sie zukünftig auf jegliche Datenübermittlungen an die KV verzichten werde, sofern die berufsrechtlichen Maßnahmen noch nicht rechtskräftig seien.

Soweit eine Verletzung der Berufspflichten noch nicht durch ein berufsgerichtliches Urteil oder eine Rüge festgestellt worden ist, dürfen Details aus den berufsrechtlichen Untersuchungsverfahren nicht an Dritte übermittelt werden.

7.2.7 Impfbuchvorlage in der Schule

Ein Gesundheitsamt forderte die Schülerinnen und Schüler der 9. Jahrgangsstufe auf, ihr Impfbuch in der Schule vorzulegen. Hintergrund sei, dass der Gesundheitsdienst die Aufgabe habe, notwendige Impfangebote für Kinder und Jugendliche und eine ausreichende Impfberatung sicherzustellen.

Um diese Aufgaben zu erfüllen, dürfen die notwendigen Daten erhoben werden. Allerdings ist die Impfbucheinsicht – ebenso wie die Impfung selbst – freiwillig und darf vom Gesundheitsdienst nicht erzwungen werden. Den betrof-

fenen Familien bleibt freigestellt, selbst zu entscheiden, ob die Kontrolle der Impfungen in der Schule durch das Gesundheitsamt oder vom eigenen Kinderarzt des Vertrauens durchgeführt werden soll.

Das Gesundheitsamt ist unserer Empfehlung gefolgt und hat das Schreiben an die Erziehungsberechtigten der betroffenen Schülerinnen und Schüler ergänzt. Nunmehr wird ausdrücklich darauf hingewiesen, dass die Impfbucheinsicht freiwillig ist, sodass nicht mehr der gegenteilige Eindruck entstehen kann. Zudem wurde das Schreiben um die entsprechenden Rechtsgrundlagen ergänzt, damit solche Missverständnisse zukünftig nicht mehr auftreten können.

Die Impfbuchdurchsicht in der Schule ist rechtmäßig, die Vorlage aber nicht verpflichtend. Die Familien können selbst entscheiden, ob sie die Impfberatung des Gesundheitsamts in Anspruch nehmen.

7.2.8 Datenerhebung im Rahmen der Qualitätssicherung

Ein Arzt beschwerte sich darüber, dass er von der KV bei einer von ihr durchgeführten Qualitätsprüfung aufgefordert worden sei, Patientendaten an die V zu übermitteln. Die KV führte aus, dass über die ausgewählten Patientinnen und Patienten Unterlagen zu durchgeführten Laborkontrollen sowie die weiteren unbedingt notwendigen Mitbehandlungen von den jeweiligen Arztpraxen angefordert würden. Insoweit sei eine Vollständigkeitskontrolle und somit eine Übermittlung der Klardaten an die KV notwendig, was auch in der Richtlinie des gemeinsamen Bundesausschusses zu Untersuchungs- und Behandlungsmethoden der vertragsärztlichen Versorgung so vorgesehen sei. Weiterhin befürchte die KV, dass bei einer Pseudonymisierung der Daten durch den verantwortlichen Arzt nicht ausgeschlossen werden könne, dass dieser die Daten manipuliere und falsche Daten an die KV übermittle.

Eine Erhebung von Patientendaten im Rahmen der Qualitätssicherung ist zulässig, diese müssen allerdings pseudonymisiert werden. Das Sozialgesetzbuch schreibt die Pseudonymisierung der Patientendaten für Zwecke der Qua-

litätssicherung ausdrücklich vor.[169] Dadurch werden diese Zwecke nicht eingeschränkt. Durch die Pseudonymisierung werden der Name sowie andere Identifikationsmerkmale durch ein anderes Kennzeichen zu dem Zweck ersetzt, die Bestimmung der Betroffenen auszuschließen oder zumindest wesentlich zu erschweren. Eine Vollständigkeitskontrolle im Hinblick auf die übermittelten Daten bleibt jedoch weiterhin möglich. Darüber hinaus besteht bei einer Übermittlung von pseudonymisierten Daten auch keine gesteigerte Gefahr, dass die übermittelnde Ärztin oder der übermittelnde Arzt die Daten manipuliert. Eine solche Manipulation ist, soweit gewollt, auch bei einer Übermittlung von Klardaten möglich.

Zwar trifft es zu, dass die „Qualitätsprüfungsrichtlinie vertragsärztliche Versorgung“ vom 18. April 2006 eine Pseudonymisierungspflicht bislang nicht ausdrücklich vorsieht. Dabei ist allerdings zu bedenken, dass die Richtlinie bereits am 1. Januar 2007 in Kraft getreten ist, die Pseudonymisierungspflicht jedoch erst am 26. Mai 2007 in das SGB V aufgenommen wurde. Die gesetzgeberische Entscheidung für eine Pseudonymisierung darf nicht dadurch umgangen werden, dass auf eine entsprechende Anpassung der Richtlinie verzichtet wird. Soweit die Richtlinie keine Pflicht zur Pseudonymisierung vorsieht, ist das rechtswidrig. Daraus folgt, dass die Richtlinie gesetzeskonform ausgelegt werden muss, solange sie nicht an das Sozialgesetzbuch angepasst worden ist. Dementsprechend dürfen nur so viele Sozialdaten erhoben werden, wie dies für die Erfüllung der jeweiligen Aufgaben erforderlich ist. Zur Qualitätsprüfung durch die KV ist eine pseudonymisierte Datenerhebung ausreichend.

Wir haben die rechtswidrige Datenerhebungspraxis der KV beanstandet. Eine abschließende Stellungnahme der KV als verantwortlicher Stelle steht noch aus.

Die Datenerhebung durch die KV bei Ärztinnen und Ärzten zur Qualitätssicherung ist zulässig, die Daten dürfen allerdings nur pseudonymisiert erhoben werden.

169 § 299 Abs. 1 SGB V

7.3 Personalwesen

7.3.1 Unsensibler Umgang mit sensitiven Daten bei Gewerkschaften

Uns erreichten mehrere Beschwerden über größere und namhafte Gewerkschaften. Beschwerdeführer waren sowohl Beschäftigte als auch Mitglieder. Alle Eingaben zeigten, dass die jeweilige Gewerkschaft überraschend unsensibel bis nachlässig mit Daten der Beschäftigten und Mitglieder umgegangen war und sich darüber hinaus den Betroffenen gegenüber zunächst uneinsichtig bis verständnislos bezüglich ihrer vorgetragenen Beschwerden zeigte.

So betraf eine Eingabe die Nutzung von Personaldaten im Rahmen des betrieblichen Eingliederungsmanagements (BEM). Nachdem die Petentin der Durchführung des BEM zugestimmt hatte und diverse Gespräche im Integrationsteam stattgefunden hatten, wurde von der Vertreterin des Arbeitgebers (der Gewerkschaft) ein Ergebnisvermerk erstellt. Dieser enthielt neben konkreten Umsetzungshinweisen auch andere Personaldaten der Betroffenen wie z.B. Angaben über einen Antrag bei einer Versicherung. Dieser Vermerk wurde ohne Kenntnis und Einverständnis der Betroffenen an Personen weitergeleitet, die zwar für die Umsetzung der vereinbarten Maßnahmen zuständig waren, aber nicht dem Integrationsteam angehörten.

Die Nutzung der Personaldaten aus dem BEM verstieß gegen § 4 Abs. 1 BDSG. Die Durchführung des BEM beruht auf dem Prinzip der Freiwilligkeit, Kooperation und Vertraulichkeit[170]. Alle Mitglieder des Integrationsteams haben über Gesprächsinhalte strikte Geheimhaltung zu wahren und sind zur Verschwiegenheit verpflichtet. Soll ein Abschluss- oder Ergebnisvermerk das Integrationsteam verlassen und an Stellen im Unternehmen weitergeleitet werden, die mit der Umsetzung der im Vermerk festgehaltenen Absprachen betraut sind, so bedarf es einer entsprechenden Freigabe durch die Betroffene oder den Betroffenen, denn sie oder er hat jederzeit und in jeder Stufe des Verfahrens die

170 § 84 Abs. 2 Sozialgesetzbuch (SGB) IX i. V. m. § 32 BDSG

Möglichkeit, das BEM zu beenden. Dies ist erst recht dann erforderlich, wenn neben dem aufgeführten Maßnahmenkatalog andere Personaldaten der oder des Betroffenen enthalten sind und weitergegeben werden sollen. Die Gewerkschaft wird dies zukünftig beachten.

Arbeitgeber haben dafür zu sorgen, dass nach Absprache mit der oder dem Betroffenen nur die Ergebnisse bzw. die geplanten Maßnahmen des BEM an die für die Umsetzung der Maßnahmen zuständigen Stellen weitergeleitet werden.

Aus der Praxis

In einem anderen Fall hatte ein Gewerkschaftsmitglied beim Kontroll- und Beschwerdeausschuss (KUB) und beim Bundesvorstand der Gewerkschaft eine Beschwerde zu erheblichen Mängeln innerhalb einer Bezirksgeschäftsführung eingereicht. Gleichzeitig zu dieser Beschwerde richtete das Mitglied ein als „Persönlich – vertraulich" gekennzeichnetes Schreiben an den Vorsitzenden der Gewerkschaft. Zu der darauf folgenden Bezirksvorstandssitzung wurde allen Mitgliedern und Ersatzmitgliedern des Bezirksvorstandes ein Hefter der kompletten Beschwerdeunterlagen des Mitglieds zugesandt. Darunter befand sich auch der als „Persönlich – vertraulich" gekennzeichnete Brief an den Vorsitzenden. Die Beschwerdeunterlagen hatte der KUB an den Bezirksvorstand weitergeleitet.

Die Weitergabe des Briefes vom Vorsitzenden an den Kontroll- und Beschwerdeausschuss sowie die Weiterleitung des Briefes und der Beschwerdeunterlagen an alle Mitglieder und Ersatzmitglieder des Bezirksvorstandes der Gewerkschaft verstießen gegen § 4 Abs. 1 BDSG, da diese Weitergabe bzw. Nutzung der personenbezogenen Daten der Beschwerdeführerin nicht erforderlich war. Insbesondere sind eindeutig als vertraulich gekennzeichnete Schreiben auch vertraulich zu behandeln. Zur weiteren Bearbeitung oder Verfolgung einer Beschwerde genügen grundsätzlich zunächst anonymisierte bzw. pseudonymisierte Daten. Dies ergibt sich auch aus dem Rechtsgedanken des § 3a BDSG, wonach personenbezogene Daten zu anonymisieren oder zu pseudonymisieren sind, soweit dies nach dem Verwendungszweck möglich und verhältnismäßig ist.

Wir haben die Verfahrensweise der Gewerkschaft bemängelt und sie aufgefordert, künftig dafür zu sorgen, dass sich derartige Vorfälle nicht wiederholen. Sie teilte uns mit, dass Beschwerden künftig nur noch pseudonymisiert bearbeitet werden und nur in Ausnahmefällen eine Einwilligung des Betroffenen eingeholt wird, sofern eine personenbezogene Bearbeitung zwingend erforderlich ist.

Der Kontroll- und Beschwerdeausschuss der Gewerkschaft sollte, soweit möglich, keine Daten von Beschwerdeführerinnen oder -führern weitergeben.

In einem anderen Fall übermittelte eine Gewerkschaft aktualisierte Kontodaten eines Mitglieds ohne dessen Kenntnis oder Einverständnis an einen von der Gewerkschaft gegründeten Verein.

Aus der Praxis

Erst nach längerem Schriftwechsel räumte die Gewerkschaft den Datenschutzverstoß ein. Sie begründete ihr Vorgehen damit, dass sowohl die Gewerkschaft als auch der Verein irrtümlich von einer einheitlichen Mitgliedschaft ausgegangenen seien und übersehen hätten, dass es sich um zwei juristisch unabhängige Unternehmen handele. Wir haben einen Verstoß gegen § 4 Abs. 1 BDSG festgestellt, da die Übermittlung der Daten ohne Rechtsgrundlage erfolgte und damit rechtswidrig war.

Auch Gewerkschaften müssen beachten, dass das Datenschutzrecht kein Verbundprivileg vorsieht.

In einer weiteren Beschwerde hatte die Personalabteilung einer Gewerkschaft eine arbeitsmedizinische Stellungnahme eines Betriebsarztes zu einer Beschäftigten an den zuständigen Betriebsrat bzw. dessen Vorsitzenden weitergeleitet, der über die Versetzung der Betroffenen beraten bzw. entscheiden wollte. Dieser versandte sodann eine Einladung an alle ordentlichen Betriebsratsmitglieder sowie Ersatzmitglieder, der die medizinische Stellungnahme als Anlage beigefügt war. Zwar enthielt das Gutachten keine konkreten Diagnosedaten, dafür jedoch Ausführungen zu Rehabilitationsmaßnahmen und Empfehlungen zu weiteren Einsatzmöglichkeiten der Betroffenen aus „orthopädischer Sicht“.

Aus der Praxis

Die Weiterleitung bzw. Nutzung der im Gutachten enthaltenen Daten war rechtswidrig.[171] Zu Gesundheitsdaten, die zu den sensitiven Daten gehören und besonders schutzwürdig sind, gehört dabei u.a. die bloße Feststellung, dass die oder der Betroffene gesund oder krank ist. Insoweit sind ärztliche Gutachten stets besonders vertraulich zu behandeln und verschlossen zur Personalakte zu nehmen. Detaillierte Auskünfte zu Leistungseinschränkungen dürfen nur in Abstimmung mit den Betroffenen an die jeweilige Personalvertretung erteilt werden. Wünschen Betroffene die Weitergabe nicht, so ist der Personalvertretung nur mitzuteilen, ob gegen den beabsichtigten Einsatz am vorgesehenen Arbeitsplatz medizinische Bedenken bestehen. Originalschreiben bzw. Gutachten dürfen dagegen keinesfalls zur Unterrichtung des Betriebsrats genutzt werden. Die Gewerkschaft wird dies zukünftig beachten.

Gewerkschaften haben als Arbeitgeber dafür zu sorgen, dass ärztliche Gutachten verschlossen zur Personalakte genommen und nicht ohne Abstimmung mit den Betroffenen z. B. an die Personalvertretung weitergeleitet werden.

7.3.2 Bewerberdaten für den Bundesfreiwilligendienst

Aus der Praxis

Ein Bürger hatte sich bei einem gemeinnützigen Verein für den neuen Bundesfreiwilligendienst (BFD) beworben. Daraufhin erhielt er ein Schreiben des Vereins mit der Bitte um Übersendung einer Kopie des letzten Schulzeugnisses sowie von Nachweisen und Arbeitszeugnissen einschließlich eines Lebenslaufs. Der Verein benutzte Bewerbungsbögen, die standardmäßig im Jugendfreiwilligendienst verwendet werden.

Die Einsatzstellen, Zentralstellen und Träger des BFD dürfen personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies für die Durchführung des Bundesfreiwilligendienstgesetzes erforderlich ist.[172] Sie dürfen personenbezogene Daten von Bewerberinnen und Bewerbern für Zwecke des Beschäf-

171 § 4 i. V. m. § 32 Abs. 1 und § 28 Abs. 6 BDSG
172 §§ 12, 8 BFDG

tigungsverhältnisses nur erheben, verarbeiten oder nutzen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist.[173] Das gilt nach Wegfall des Zivildienstes auch für Bewerberinnen und Bewerber des BFD. Die Abfrage von Bewerberdaten darf nur im Hinblick auf den konkret vorgesehenen Diensteinsatz erfolgen. Eine pauschale Datenabfrage steht dazu im Widerspruch. Dabei ist der Aussagegehalt von Schulzeugnissen und somit deren Erforderlichkeit – anders als im Jugendfreiwilligendienst – insbesondere bei älteren Bewerberinnen und Bewerbern für die Frage der Einsatzmöglichkeiten beim BFD sehr gering. Allenfalls der sog. Zeugniskopf kann bei jüngeren Bewerbern für die Eignung zum BFD relevante Informationen (z.B. zu Fehlzeiten und Sozialverhalten) enthalten, einzelne Schulnoten sind hingegen regelmäßig nicht erforderlich. Der Verein sicherte zu, den Fragebogen zeitnah zu überarbeiten.

Die jeweilige Einsatzstelle für den Bundesfreiwilligendienst darf vom Bewerber nur die Daten erheben, die zur Begründung eines Diensteinsatzes erforderlich sind.

7.3.3 Beschäftigtenblut

Dem Landesamt für Gesundheit und Soziales (LAGeSo) war bei einem Genehmigungsverfahren zu einer genetischen Forschung aufgefallen, dass eine Professorin der Charité Blutproben ihrer Angestellten für ihre Forschung nutzen wollte. Jeweils vier Blutproben sollten vor ihrer Verwendung zur Forschung zusammengefügt und auf HIV/AIDS und Hepatitis geprüft werden. Die Angestellten hätten dem Projekt zugestimmt.

Eine Nutzung von Beschäftigtendaten für Forschungszwecke ist grundsätzlich rechtswidrig, da sie für die Durchführung des Arbeitsverhältnisses nicht erforderlich ist und zudem das schutzwürdige Interesse der Betroffenen am Ausschluss dieser Nutzung in aller Regel überwiegt. Zu berücksichtigen ist auch, dass die Information, dass keiner der vier Angestellten unter einer bestimmten

173 § 4 Abs. 1 i. V. m. § 32 Abs. 1 BDSG

Krankheit leidet, ebenso als sensitives Datum einzustufen ist wie das Ergebnis, zu einer so kleinen Gruppe zu gehören, von der mindestens einer eine bestimmte Krankheit hat. Die Freiwilligkeit der Einwilligung der Betroffenen war aufgrund ihres Abhängigkeitsverhältnisses nicht gegeben. Es gelang uns mit Hilfe des LAGeSo, die Charité zum Verzicht auf diese Untersuchung zu bewegen.

Medizinische Forschungsprojekte mit Daten von Beschäftigten sind grundsätzlich nicht gestattet. Dies gilt in jedem Fall für Blutanalysen.

7.4 Wohnen und Umwelt

7.4.1 Smart Metering: Wie intelligent dürfen Stromzähler werden?

Aus der Praxis

Das intelligente Stromnetz, das sog. Smart-Grid, soll im Rahmen der Klimaschutzpolitik dazu beitragen, die Energieeffizienz zu steigern. Der intelligente Stromzähler, das Smart Meter, wird die Technologie sein, die den Verbrauchenden dabei am meisten auffällt. Sie ermöglicht ihnen, den eigenen Verbrauch zu kontrollieren und zu regulieren, und den Energieversorgern eine bedarfsgerechte Versorgung. Die digitale Messung des Energieverbrauchs der Haushalte birgt aber auch Gefahren für die Persönlichkeitsrechte der Betroffenen.

Wenn der Energieverbrauch detailliert erfasst sowie langfristig aufgezeichnet wird, derartige Verbrauchsprofile mit anderen Daten verknüpft und die Daten per Fernzugriff ausgelesen werden können, drohen tiefgreifende Verletzungen der Persönlichkeitsrechte der Verbraucherinnen und Verbraucher.[174] Anhand der von den intelligenten Stromzählern gelieferten Daten ist es nicht nur möglich nachzuvollziehen, z.B. welche Haushaltsgeräte zu einem bestimmten Zeitpunkt

174 Vgl. JB 2009, 1.1.1

in Betrieb sind, sondern auch, von welcher Marke und welchem Typ sie sind. Es ist bei modernen Fernsehgeräten sogar möglich, auf die geschauten Fernsehprogramme zu schließen, weil unterschiedliche Helligkeitswerte zu unterschiedlichen Stromverbräuchen führen. Zudem wird die Kontrolle erschwert, inwieweit die eigenen Verbrauchsdaten offenbart werden, da durch die neuen Messsysteme eine Fernmessung möglich wird, die so stattfinden kann, dass die Verbraucherinnen und Verbraucher sie weder erkennen noch daran mitwirken können. Deshalb hatten die Datenschutzbeauftragten 2010 gesetzliche Regelungen zur Begrenzung der Erhebung von Verbrauchsdaten gefordert.[175]

Im Juli 2011 wurde das Energiewirtschaftsgesetz novelliert und eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten aus dem intelligenten Messsystem eingefügt. Aufgrund unserer Initiative hat Berlin einen Antrag im Bundesrat gestellt, der einstimmig angenommen worden ist. Der Bundesrat hat zusätzliche Maßnahmen vorgeschlagen und darum gebeten zu prüfen, ob die datenschutzrechtlichen Regelungen ausreichen, um die Persönlichkeitsrechte der Betroffenen gegen eine Ausforschung des Nutzerverhaltens zu schützen.[176] Einige zentrale Punkte, die wir über den Bundesrat in das Gesetzgebungsverfahren eingebracht haben, sind in das Gesetz eingegangen. So darf die Belieferung mit Energie nicht von der Angabe nicht erforderlicher personenbezogener Daten abhängig gemacht werden. Fernmessen und Fernwirken sind nur mit Einwilligung der zuvor informierten verbrauchenden Person zulässig. Ihr werden hierfür Kontroll- und Einwilligungsmöglichkeiten eingeräumt.[177] Das Gesetz sieht zudem Rechtsverordnungen, Schutzprofile und technische Richtlinien für Messsysteme vor, in denen die Einzelheiten näher geregelt werden sollen.

Entwürfe der Schutzprofile für die Kommunikationseinheit (Gateway) für Smart Meter[178] und für das Sicherheitsmodul der Smart Meter[179] sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht wor-

175 Vgl. Dokumentenband 2010, S. 19
176 Vgl. BR-Drs. 343/4/11; BT-Drs. 17/6248
177 § 21 Abs. 6 EnWG
178 Protection Profile for the Gateway of a Smart Metering System, www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html
179 Protection Profile for the Security Module of a Smart Metering System, https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Security/security_module_node.html

den. Über den Gateway wird die gesamte Kommunikation zwischen den drei beteiligten Netzen geführt:

- Das **Fernbereichsnetz (Wide Area Network – WAN)** verbindet über weite Entfernungen eine Vielzahl von Kommunikationseinheiten zur Synchronisierung von Stromverbrauch und Stromerzeugung, Übertragung von Abrechnungsdaten und Administration der mit ihm verbundenen lokalen Netze.
- Das **Heimnetzwerk (Home Area Network – HAN)** verbindet die Energie verbrauchenden Geräte und ggf. Energie erzeugenden Systeme einer bewohnten Einheit (Haus, Wohnung). Es wird für Zwecke des Energiemanagements verwendet, z.B. zur Steuerung von Zeit und Höhe des Energieverbrauchs und der Energieeinspeisung aufgrund von Steuerungssignalen oder Tarifstatusdaten aus dem WAN.
- Das **lokale Messnetz (Local Metrological Network – LMN**) verbindet die lokalen Messsysteme zur Sammlung und Übertragung von Messdaten an das WAN.

Der zentrale Anknüpfungspunkt für die Sicherstellung der Informationssicherheit im künftigen Energieinformationsnetz (Smart Grid) ist der Gateway, da über ihn alle Daten fließen, die aus den Privathaushalten gewonnen werden oder in sie hineinfließen, die für die Abrechnung und – vor allem – Energiebedarfssteuerung im Smart Grid erforderlich sind. Die in das WAN herausfließenden Daten haben einen hohen Schutzbedarf bzgl. der Vertraulichkeit und der Integrität, weil sie personenbezogen sein können. Die in das HAN hineinfließenden Daten haben einen hohen Schutzbedarf hinsichtlich der Integrität und der Verfügbarkeit, da Fehlfunktionen oder Ausfälle in der Steuerung der im HAN befindlichen Geräte erhebliche Folgen für die Sicherheit der Menschen zur Folge haben können.

Für die Umsetzung der Schutzprofile durch die Hersteller entwickelt das BSI derzeit eine „Technische Richtlinie Smart Meter“. Dazu gehören drei Anlagen mit kryptografischen Vorgaben für die Infrastrukturen von Messsystemen,

Anforderungen an die Interoperabilität des Sicherheitsmoduls und für die Public Key Infrastruktur für Smart Meter Gateways.[180]

Die Datenschutzbehörden des Bundes und der Länder erstellen derzeit ein Eckpunktepapier, in dem mögliche Datenschutzprobleme aufgezeigt und Lösungen vorgestellt werden. Wir entwickeln Vorgaben und Empfehlungen für die datenschutzgerechte Gestaltung der intelligenten Stromzähler. Auch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group") hat zahlreiche Schutzmechanismen empfohlen.[181]

7.4.2 Das Stadtmodell der Senatsverwaltung für Stadtentwicklung im Internet

Die Senatsverwaltung für Stadtentwicklung veröffentlicht im Internet zur Demonstration der Bautätigkeit in der Berliner Innenstadt eine Stadtmodelldatenbank. Zu den jeweiligen Gebäuden, die mit Straße und Hausnummer aufgeführt sind, werden Bilder und Pläne publiziert. Zudem werden die Architekten und Bauherren benannt sowie Einzelheiten in Bezug auf das Grundstück und das Gebäude angegeben wie die Nutzung, die (überbaute) Fläche oder die Bauart. Die Daten erfragt die Senatsverwaltung für Stadtentwicklung bei den Architekten.

Nicht nur bei den Angaben zu den Architekten und Bauherren, sondern auch in Bezug auf das Grundstück und dessen Bebauung handelt es sich aufgrund der hausnummerngenauen Angabe um personenbezogene Daten. Dies gilt jedenfalls, soweit architektonische Besonderheiten wiedergegeben werden, die unveränderbar oder dauerhaft sind, da hierdurch auch Informationen zu den aktuellen Wohn- und Eigentumsverhältnissen gegeben werden.

180 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (TR-03109), https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html

181 Vgl. Dokumentenband 2011, S. 124

Für die Erhebung der Daten und deren Veröffentlichung im Internet fehlt eine Rechtsgrundlage. Die Senatsverwaltung für Stadtentwicklung muss daher vor allem für die Veröffentlichung der Projektdaten die Einwilligungen der Architekten, Bauherren und Grundstückseigentümer einholen. Diese sind über die Bedeutung der Einwilligung und den Verwendungszweck der Daten aufzuklären und insbesondere auf die Freiwilligkeit der Einwilligung hinzuweisen.[182] Für die bereits veröffentlichten Projekte sind die Einwilligungen unverzüglich nachzuholen.

Die Senatsverwaltung für Stadtentwicklung hat entsprechend unseren Forderungen Hinweise zur Bedeutung und Freiwilligkeit der Einwilligungen aufgenommen und mit unserer Unterstützung die Formulare überarbeitet. Die Einwilligungserklärungen für die älteren Projekte werden sukzessive eingeholt. Zudem werden die betroffenen Eigentümer und Mieter auf der Internetseite über ihr Widerspruchsrecht in Bezug auf die Veröffentlichung der Fotos informiert.

Die Stadtmodelldatenbank ist nun auf einem datenschutzkonformen Weg.

7.4.3 Neue Entwicklungen bei Panoramadiensten

Aus der Praxis

Nach Google Street View ist der Geodatendienst Microsoft Bing Maps Streetside online gegangen. In Reaktion auf die Verpixelungen bei Street View entstand zudem ein Online-Angebot, bei dem auf einem Online-Kartensystem die bei Street View unkenntlichen Häuser gekennzeichnet werden konnten. Auf einer damit verlinkten Webseite konnten Nutzende Fotos der Häuser, die bei Street View verpixelt sind, einstellen und sie damit wieder sichtbar machen.

Einige dieser Bilder waren mit Straße und Hausnummer des abgebildeten Hauses betitelt. Bei diesen Fotos handelte es sich um personenbezogene Daten, da sie der Gebäudeadresse und damit dem Grundstückseigentümer sowie den

182 § 6 Abs. 3 – 5 BlnDSG

Bewohnern zugeordnet werden konnten.[183] Für die Veröffentlichung dieser Daten fehlt eine Rechtsgrundlage.[184] Zudem sind die Interessen der Betroffenen zu berücksichtigen, die bereits der Veröffentlichung der Abbildungen bei Google Street View widersprochen haben. Sie haben durch ihren Widerspruch deutlich gemacht, dass die Bilder ihrer Häuser nicht veröffentlicht werden sollen.

Dieser Rechtslage hätte z.B. dadurch Rechnung getragen werden können, dass die Angabe von Straße und Hausnummer zu den einzelnen Fotos entfernt oder dass auch hier den Betroffenen ein Widerspruchsrecht eingeräumt würde, das z.B. durch Entfernen des Bildes oder der Angabe von Straße und Hausnummer zu dem Bild berücksichtigt werden könnte. Nachdem wir entsprechende Hinweise erteilt haben, sind die beiden Webseiten deaktiviert worden.

Auch Microsoft hatte auf Druck der Datenschutzaufsichtsbehörden für den Geodatendienst Bing Maps Streetside eine Vorabwiderspruchsmöglichkeit eingeräumt. Gesichter und Autokennzeichen macht Microsoft auf den Bildern automatisch unkenntlich. Ein Widerspruch ist auch noch nach Veröffentlichung der Bilder der Hausansichten möglich.[185] Dagegen ist die im BITKOM-Datenschutz-Kodex für Geodatendienste als Selbstverpflichtung der Wirtschaft für Panorama-Bilderdienste eingeräumte Widerspruchsmöglichkeit *nach* Veröffentlichung der Panoramabilder nicht ausreichend, da schon mit der Veröffentlichung das Recht auf informationelle Selbstbestimmung verletzt ist.

Für georeferenzierte Panoramadienste ist die Veröffentlichung der Aufnahmen ohne die Möglichkeit des Vorabwiderspruchs rechtswidrig.

183 Vgl. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008: Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet; Dokumentenband 2008, S. 37

184 § 59 Abs. 1 UrhG (sog. Panoramafreiheit) und § 23 Abs. 1 Nr. 2 KunstUrhG stellen keine Erlaubnisnormen i. S. d. § 4 Abs. 1 BDSG dar; denn diese Vorschriften des Zivilrechts gewährleisten keinen dem BDSG vergleichbaren Datenschutz.

185 Vgl. unsere Presseerklärung vom 15. August 2011: Bing Maps Streetside: Vorabwiderspruch bei Microsoft bis 30. September 2011 einlegen!

7.4.4 Fördermittel nur bei Vorlage von Führungszeugnissen

Aus der Praxis

Ein freier Jugendhilfeträger bat uns zu prüfen, ob die Senatsverwaltung für Stadtentwicklung im Rahmen der Bewilligung und Verwendung von Projektfördermitteln aus dem Quartierfonds 1 und 2 im Programm „Zukunftsinitiative Stadtteil“ von den geförderten Stellen die Vorlage erweiterter Führungszeugnisse[186] von am Projekt beteiligten Personen verlangen darf.

Nach dem Berliner Datenschutzgesetz[187] ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Es ist keine Rechtsgrundlage ersichtlich, die eine solche Datenübermittlung an die Senatsverwaltung rechtfertigen könnte. Das Sozialgesetzbuch Achtes Buch[188] ermächtigt lediglich die Träger der öffentlichen Jugendhilfe, sich von den betroffenen Personen ein erweitertes Führungszeugnis vorlegen zu lassen. Das Bundeszentralregistergesetz[189] enthält nur eine Berechtigung der oder des Betroffenen, das eigene Führungszeugnis anzufordern. Mit dem Berliner Rahmenvertrag für Hilfen in Einrichtungen und durch Dienste der Kinder- und Jugendhilfe (BRVJug) werden die Vorgaben des § 72a Satz 3 SGB VIII umgesetzt. Er gilt allerdings nicht für die Senatsverwaltung für Stadtentwicklung.

Zukünftig werden sich die geförderten Projektgruppen auf unsere Empfehlung hin die erweiterten Führungszeugnisse der Beschäftigten vorlegen lassen und der Senatsverwaltung für Stadtentwicklung zusichern, dass diese keine positiven Eintragungen hinsichtlich der im Bundeszentralregistergesetz[190] abschließend aufgezählten Delikte beinhalten. Die jetzt gefundene Regelung zur Prüfung der Eignung einer Person für die Wahrnehmung von Aufgaben in der Kinder- und Jugendhilfe wird den Interessen aller Beteiligten gerecht.

Fördermittel dürfen nicht von der Vorlage erweiterter Führungszeugnisse abhängig gemacht werden.

186 § 30 a Bundeszentralregistergesetz (BZRG)
187 § 6 Abs. 1 BlnDSG
188 § 72a SGB VIII
189 § 30 a Abs. 1 Nr. 2 b) und c) BZRG
190 § 32 Abs. 5 BZRG

8. Wissen und Bildung

8.1 Statistik, Wissenschaft, Archivwesen und Bibliotheken

8.1.1 Das Jahr des „Zensus 2011“

Im Rahmen der aktuellen Volkszählung „Zensus 2011“ sind Bürgerinnen und Bürger für die Gebäude- und Wohnungszählung und die Haushaltsstichprobe mittels Fragebogen direkt befragt worden.[191] Wir haben daher die Erhebungsstelle Berlin und die Durchführung des „Zensus 2011“ im Amt für Statistik Berlin-Brandenburg einer datenschutzrechtlichen Kontrolle unterzogen.[192]

Aus der Praxis

Die Erhebungsstelle Berlin unterstützt das Amt für Statistik Berlin-Brandenburg bei der Durchführung des „Zensus 2011“.[193] Sie führt die stichprobenartige Haushaltsbefragung und die Erhebung in Sonderbereichen (z.B. Krankenhäusern, Haftanstalten) durch und ist für den Einsatz der Erhebungsbeauftragten verantwortlich. In Bezug auf den Einsatz von Erhebungsbeauftragten und den Umgang mit den Fragebogen haben wir insbesondere für zukünftige Erhebungen Empfehlungen zur Verbesserung gegeben. So sollten vor allem die Ausweise der Erhebungsbeauftragten nicht deren Privatanschrift enthalten und präzise Vorgaben für die Abgabe der Fragebogen durch die Erhebungsbeauftragten gelten.

Zudem haben wir das IT-Sicherheitskonzept und die Umsetzung der IT-Sicherheitsmaßnahmen beim „Zensus 2011“ überprüft. Positiv hervorzuheben ist, dass bei der Erstellung des IT-Sicherheitskonzeptes die Vorgehensweise nach IT-Grundschutz und die Vorgaben des Bundesamtes für Sicherheit in der

191 Vgl. JB 2010, 9.1.4

192 Die Kontrolle erfolgte im Auftrag der für das Amt zuständigen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg.

193 Vgl. § 10 ZensG 2011

Informationstechnik[194] konsequent eingehalten wurden. Das IT-Sicherheitskonzept ist grundsätzlich geeignet, die mit der Verarbeitung personenbezogener Daten beim „Zensus 2011“ verbundenen Risiken zu beherrschen. Jedoch sind einige Nachbesserungen erforderlich, insbesondere die Betrachtung aller erforderlichen Grundschutzbausteine. Des Weiteren konnten wir bewirken, dass die von den Meldebehörden an das Amt für Statistik übermittelten Dateien mit den Übermittlungssperren zu Meldedatensätzen[195] frühzeitig gelöscht wurden

.

Die Datenschutzbeauftragten des Bundes und der Länder wollen im Nachgang zum „Zensus 2011“ Empfehlungen zur Verbesserung des Datenschutzes für zukünftige Volkszählungen aussprechen. Aktuell ist insbesondere die zeitnahe Löschung der erhobenen Daten in den Statistischen Landesämtern zu überwachen.

8.1.2 Wem „gehören“ die Daten aus klinischen Prüfungen?

Aus der Praxis

Eine Professorin und Leiterin einer klinischen Prüfung nahm vor ihrem Ausscheiden aus den Diensten der Sponsorin schriftliche und elektronische Studienunterlagen in Kopie für die weitere Forschung bei ihrem zukünftigen Arbeitgeber an sich. Gesammelte Blutproben wurden in ein anderes Forschungsinstitut verbracht. Zwar wurde – ohne die Zustimmung der Sponsorin – versucht, die Einwilligung von Betroffenen für die weitere Auswertung der Studiendaten und der Blutproben in anderen Prüfungszentren einzuholen. Dies erfolgte aber nicht in der für solche Verfahren üblichen Schriftform mit eigenhändiger Unterschrift der Probanden.

Die medizinische Forschung mit Probanden ist ein klassisches Anwendungsgebiet des Datenschutzrechts, da die Forschenden typischerweise in Kontakt mit sensitiven personenbezogenen Daten kommen. Diese Gesundheitsdaten genießen nach den Datenschutzgesetzen einen hohen Schutz. Daher wiegen

194 BSI-Standards 100-2 und 100-3
195 Vgl. JB 2010, 9.1.4

Datenschutzverletzungen in diesem Bereich besonders schwer. Dies gilt auch bei klinischen Prüfungen, die der Erforschung von Wirkungen und Nebenwirkungen von Arzneimitteln mit dem Ziel dienen, sich von deren Wirksamkeit oder Unbedenklichkeit zu überzeugen. Solche Prüfungen sind Voraussetzung für die Zulassung von Arzneimitteln. Um den Probanden einen möglichst hohen Schutz zu bieten, sieht das Arzneimittelgesetz und die sich darauf stützende Verordnung über die Anwendung der Guten Klinischen Praxis (GCP-Verordnung) ein streng formalisiertes Verfahren bei der Beantragung und Durchführung von klinischen Prüfungen vor. Verantwortlich für die Organisation und Finanzierung der Prüfung ist der sog. Sponsor, der – soweit er seinen Sitz in Berlin hat – unserer datenschutzrechtlichen Kontrolle unterliegt.

Im Frühjahr 2010 erhielten wir von der Leitung der Charité – Universitätsmedizin Berlin (Charité) Kenntnis von einer seit 2007 dort durchgeführten klinischen Prüfung zur Behandlung von Patienten mit Multipler Sklerose. Mehr als 100 Betroffene wurden in die Untersuchung mit einbezogen. Ihnen wurde u. a. eine Prüfsubstanz verabreicht, wobei entsprechende Studiendaten schriftlich und elektronisch erstellt, regelmäßig Blutproben entnommen und Darstellungen aus Kernspintomographie und EKG gespeichert wurden. Die Speicherung dieser Daten sollte nach den Probandeninformationen und den Antragsunterlagen für das erforderliche Ethikvotum ausschließlich in den Räumlichkeiten der Charité und zwei weiteren Prüfungszentren erfolgen. Die Ethikkommission des Landes Berlin gab der Studie im Vorfeld der Untersuchung auf Grundlage der eingereichten Antragsunterlagen und im Einklang mit den Regelungen des Arzneimittelgesetzes ein positives Votum.

Wegen der eigenmächtigen Vervielfältigung der Studienunterlagen und der Verbringung der Blutproben an einen vom Prüfungsplan nicht vorgesehenen und von den Patienteninformationen abweichenden Ort haben wir Strafantrag bei der Staatsanwaltschaft gestellt. Es bestand der Verdacht eines unbefugten Abrufens und eines Sich-Verschaffens von personenbezogenen Daten, die nicht offenkundig waren.[196]

Die Staatsanwaltschaft stellte das Strafverfahren jedoch zunächst mit der Begründung ein, dass ein unbefugtes Handeln der Wissenschaftlerin nicht ange-

196 § 32 Abs. 1 Nr. 2 BlnDSG

nommen werden könne, da sie zum Zeitpunkt der Tathandlungen noch Leiterin der Studie gewesen sei. Die Gegenvorstellung unseres Hauses, dass das neue Forschungsinstitut zu keinem Zeitpunkt als Prüfungszentrum der Studie vorgesehen war, wies die Staatsanwaltschaft zurück, nunmehr mit der Begründung, dass der erforderliche Vorsatz der Professorin zu einem „unbefugten" Handeln gefehlt habe. Dennoch verstieß der Umgang mit den Patientendaten gegen das Datenschutzrecht. Wir haben die Leitung der Forschungseinrichtung gebeten, alle dort tätigen Personen auf die Rechtslage hinzuweisen.

Die Nutzung von Biomaterial für Forschungszwecke außerhalb der in den Betroffeneninformationen benannten Prüfungszentren ohne die Einwilligung der Betroffenen ist datenschutzrechtlich grundsätzlich unzulässig. Darin liegt regelmäßig eine grobe Missachtung des informationellen Selbstbestimmungsrechts der Betroffenen, welches auch den Ort der Verarbeitung der eigenen Daten umfasst. Die personenbezogenen Daten aus klinischen Prüfungen „gehören" weder dem Sponsor noch den Prüfern, sondern allein den Betroffenen. Sie bestimmen über den Umfang und die Art der Verwendung.

8.1.3 Nationale Kohorte

Aus der Praxis

Die „Nationale Kohorte" bezeichnet eine großangelegte epidemiologische Forschungsstudie zur Untersuchung von Volkskrankheiten wie Krebs, Diabetes oder verschiedenen Herz-Kreislauferkrankungen[197]. Das Besondere an der Studie ist die große Anzahl der geplanten Studienteilnehmenden sowie die lange Laufzeit von 10 bis 20 Jahren. Dadurch erhoffen sich die Wissenschaftlerinnen und Wissenschaftler wertvolle Erkenntnisse über die Zusammenhänge von genetischen Faktoren, Umweltbedingungen, sozialem Umfeld und Lebensstil bei der Entstehung von Krankheiten. Zugleich sollen Vorbeugungs- und Früherkennungsmöglichkeiten verbessert werden. Die Untersuchungen und die regelmäßigen Nachuntersuchungen werden

197 „Kohortenstudien" sind wissenschaftliche Längsschnittuntersuchungen, bei denen eine Gruppe (Kohorte) von Probanden über einen längeren Zeitraum beobachtet und untersucht wird.

Befragungen zu persönlichen Verhältnissen ebenso umfassen wie die Entnahme von Blutproben und ggf. anderem Biomaterial. An der Studie werden sich in ganz Deutschland insgesamt 18 Studienzentren beteiligen. Verantwortlich für die Durchführung der Studie wird ein Verein „Nationale Kohorte e. V." sein. Der Beginn der Hauptuntersuchung ist für 2012 vorgesehen.

Ein wesentlicher Teil der Vorplanung zur Nationalen Kohorte war die Durchführung von sog. Pretests, d. h. Versuchen zur Überprüfung der Machbarkeit, wissenschaftlichen Qualität und voraussichtlichen Kosten der nachfolgenden Hauptstudie. Diese Pretests wurden im Raum Berlin als Verbundprojekt durch das wissenschaftliche Cluster Berlin-Brandenburg durchgeführt, bestehend aus dem Max-Delbrück-Centrum als Koordinationsstelle, der Charité Universitätsmedizin Berlin, dem Deutschen Institut für Ernährungsforschung und dem Robert-Koch-Institut als unterstützende Einrichtung. Dabei wurden insgesamt 300 Personen aus der Allgemeinbevölkerung (Basisprogramm) sowie weitere 600 aus der Türkei stammende Personen befragt und untersucht. Die Auswahl der Teilnehmenden erfolgte im ersten Schritt über eine Melderegisterauskunft, mit der eine zufällige Personengruppe von insgesamt 102.000 Bewohnerinnen und Bewohnern ermittelt wurde. In der Folge wurden 2.000 von den Ermittelten unmittelbar mit Anschreiben und Telefonanrufen zur Teilnahme an den Pretests gebeten. Die übrigen 100.000 Datensätze wurden mit einem onomastischen Programm zur Namensanalyse auf die ethnische Abstammung der betroffenen Personen untersucht. Auf diese Weise konnten die 600 benötigten, aus der Türkei stammenden Probanden für die Pretests gewonnen werden.

Die Konzeption des Vorhabens war von dem deutlichen Bemühen getragen, den Anforderungen des Datenschutzes umfassend Rechnung zu tragen. Allerdings waren auch Nachbesserungen an den Probandeninformationen bezüglich des genauen Forschungszwecks nötig. Der „Pretest"-Charakter des Vorhabens musste in den Informationen deutlicher zu Tage treten, um den Voraussetzungen einer rechtswirksamen informierten Einwilligung zu genügen.

Keinen rechtlichen Einwänden begegnete hingegen die Verwendung der Melderegisterdaten zur onomastischen Auswertung. Denn nach § 25 Abs. 1 Satz 4 Berliner Meldegesetz (MeldG) ist eine Datenübermittlung von einer Vielzahl nicht namentlich bezeichneten Einwohnern an öffentliche Stellen stets zulässig,

sofern für die Zusammenstellung der Personengruppe nur diejenigen Daten zugrunde gelegt werden, welche ohnehin im Rahmen einer Einzelabfrage übermittelt werden dürften. Die ethnische Abstammung einer Person gehört zwar nicht zu diesen Daten. Die einschränkende Voraussetzung der Vorschrift bezieht sich jedoch nicht auf eventuelle Auswertungen bei den Empfängern der Melderegisterdaten, sondern auf Zusammenstellungen bei der Meldebehörde selbst. Dies hat den Hintergrund, dass eine Übermittlung von Datensätzen, die nach einem bestimmten Kriterium geordnet sind, das selbst nicht Gegenstand einer Einzelabfrage sein könnte, unzulässig ist, da ansonsten indirekt dieses Datum preisgegeben würde. Nähme man z.B. an, dass der Migrationshintergrund von Einwohnerinnen und Einwohnern im Melderegister erfasst sein würde, so könnte der Empfänger der Melderegisterdaten nicht in zulässiger Weise eine Auskunft über alle Einwohnerinnen und Einwohner mit Migrationshintergrund verlangen, da nach § 25 Abs. 1 Satz 4 MeldeG eine Gruppenbildung nach diesem Merkmal unzulässig ist.

Bei der Durchführung der Pretests zeigte sich eine unerwartet niedrige Teilnahmebereitschaft der zur Studie eingeladenen Personen. Es stand zu befürchten, dass keine 300 Personen aus der Allgemeinbevölkerung für das Basisprogramm zu gewinnen waren. Deshalb wandten sich die Forscher an uns mit der Frage, ob es mit den Vorschriften des Datenschutzes vereinbar sei, aus den Datensätzen der rund 94.000 nicht aus der Türkei stammenden Betroffenen, die nach der onomastischen Auswertung verblieben waren, eine Aufstockungsstichprobe für das Basisprogramm zu entnehmen. Dies war zulässig, da Nachteile für das informationelle Selbstbestimmungsrecht der Betroffenen in diesem frühen Vorbereitungsstadium der Forschungstätigkeit nicht zu befürchten waren und sich weiterhin keine Besonderheiten in Bezug auf die Datensicherheit ergaben.

Die Übermittlung von Melderegisterdaten durch die Meldebehörde ist zulässig, wenn Zweck der Übermittlung eine Selektion der Datensätze nach der ethnischen Herkunft der Betroffenen ist, die für ein Forschungsprojekt gewonnen werden sollen. Auch sind Änderungen an der Ausgestaltung eines Forschungsvorhabens in datenschutzrechtlicher Hinsicht zulässig, wenn damit keine Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sind und sich keine Besonderheiten in Bezug auf die Datensicherheit ergeben.

8.1.4 Studentenwerk Berlin I und II

Antrag auf Gehaltsunterdrückung beim BAföG

Das Studentenwerk Berlin wies in einem BAföG-Bescheid an einen Studenten das Gehalt der Eltern aus, denn ihr Antrag auf Gehaltsunterdrückung wurde versehentlich nicht berücksichtigt. Unsere Mangelfeststellung hat nicht zu einer Änderung des nächsten BAföG-Bescheids an den Studenten geführt. Das Studentenwerk Berlin meinte, dass die bloße Wiederholung einer unzulässigen Datenübermittlung selbst nicht unzulässig sein könne.

Die Überprüfung einer Beschwerde der Eltern des BAföG-Empfängers ergab, dass deren Antrag auf Einkommensunterdrückung[198] im Förderungsantrag nicht berücksichtigt worden ist. Die Bekanntgabe der Einkommensverhältnisse der Eltern war von keiner rechtlichen Grundlage gedeckt. Es lag damit ersichtlich ein Verstoß gegen den Datenschutz vor, den wir gegenüber dem Studentenwerk festgestellt haben. Der Hinweis des Studentenwerks, dass die Angaben über die Einkünfte der Eltern nicht mehr „zu schützen" gewesen seien, da die besagten Angaben ohnehin aufgrund der Bescheidung über einen Vorzeitraum gegenüber dem Geförderten bekannt gegeben worden waren, war hierbei ohne Belang. Es ist grundsätzlich im Rahmen der Gesetze jedermann selbst überlassen, über Art und Umfang der Weitergabe und Nutzung seiner Daten zu bestimmen.

Im folgenden BAföG-Bescheid an den Studenten wurde trotz unserer Mangelfeststellung erneut das Einkommen der Eltern bekanntgegeben. Dies erfolgte, obwohl die Eltern im Antragsformular und in einem gesonderten Schreiben darauf hingewiesen hatten, dass sie ihren Widerspruch gegen die Bekanntgabe des Einkommens aufrechterhalten. Das Studentenwerk begründete die Bekanntgabe damit, dass der neue Bescheid keine eigenständige Regelungswirkung enthalte, sondern lediglich der Klarstellung diene. Diese Auffassung hält einer rechtlichen Prüfung jedoch nicht stand.

198 § 35 Abs. 1 SGB I i.V. m. § 50 Abs. 2 Satz 3 Bundesgesetz über individuelle Förderung der Ausbildung (BAföG)

Die Wiederholung einer rechtswidrigen Übermittlung ist selbst rechtswidrig.

Autoload-Verfahren

Wir stellten fest, dass das Studentenwerk Berlin im Rahmen des sog. „Autoload-Verfahrens" die Studierenden in unzureichender Weise über die Verwendung ihrer Bankdaten informiert hatte. Ein verfahrensspezifisches Sicherheitskonzept existierte nicht.

Nachdem wir einen Hinweis eines studentischen Vertreters der Technischen Universität Berlin erhalten hatten, überprüften wir das neu eingerichtete „Autoload-Verfahren" des Studentenwerks. Im „Autoload-Verfahren" bezahlen die Studierenden mit ihrer Mensakarte, wobei ein vorher bestimmter Betrag per Lastschrift von ihren Bankkonten abgebucht wird. Die Kontodaten werden im Kassensystem des Studentenwerks erfasst und bei einem Aufladungswunsch der Studierenden automatisch zur Abbuchung im Lastschriftverfahren verwendet. Es stellt damit eine Alternative zu den in den Mensen aufgestellten Aufwertern dar, die für das Einzahlen von Bargeld genutzt werden können. Die Prüfung ergab, dass die Studierenden weitestgehend im Unklaren über den Verbleib und die exakte Verwendung der Kontodaten beim „Autoload-Verfahren" gelassen wurden. Wir forderten das Studentenwerk daher dazu auf, das den Studierenden an den Mensa-Kassen vorgelegte und sodann von diesen auszufüllende Formular aus Gründen der Transparenz zu überarbeiten. Darüber hinaus sollten gut sichtbare Aushänge in den Mensen und Cafeterien angebracht werden, die über die verschiedenen Möglichkeiten des bargeldlosen Bezahlens informieren. Diesen Aufforderungen kam das Studentenwerk nach. Gegenwärtig wird es bei der Anfertigung des Sicherheitskonzepts von uns beraten.

Öffentliche Stellen des Landes Berlin sind verpflichtet, für Verfahren der automatisierten Datenverarbeitung ein verfahrensspezifisches Sicherheitskonzept vorzuhalten, auf dessen Grundlage eine Entscheidung über die zu treffenden technischen und organisatorischen Maßnahmen möglich ist. Dies gilt auch für solche Verfahren, bei denen ein bestimmter Betrag per Lastschrift automatisch von den Bankkonten der Betroffenen abgebucht wird.

8.1.5 Novellierungsbedarf im Landesarchivgesetz

Immer wieder erreichen uns Anfragen des Landesarchivs, der Presse, aber auch von betroffenen und interessierten Bürgerinnen und Bürgern, die die Möglichkeiten der Nutzung von Archivgut betreffen. Es enthält oft zahlreiche personenbezogene Daten von lebenden oder verstorbenen Personen.

Die einzelnen Fälle zeigen, dass das Verhältnis des Gesetzes über die Sicherung und Nutzung von Archivgut des Landes Berlin (Archivgesetz) zum Berliner Datenschutzgesetz und zum Berliner Informationsfreiheitsgesetz verschiedene Fragen aufwirft, die eine grundsätzliche Novellierung des Archivgesetzes dringend erforderlich machen. Berlin hat 1993 als erstes Bundesland Regelungen zum Datenschutz in sein Archivgesetz aufgenommen. Sowohl das Archivrecht als auch die Technik haben sich inzwischen so weiterentwickelt, dass das Berliner Archivgesetz dem angepasst werden sollte. Anzustreben ist dabei eine Vereinheitlichung mit den Regelungen in den Archivgesetzen des Bundes und anderer Bundesländer. Dabei sollten die Schutzfristen der längeren Lebenserwartung der Menschen angepasst werden.[199]

Für die Nutzung von Archivgut, das nach seinem wesentlichen Inhalt Personen betrifft, hat der Gesetzgeber eine Abwägung der maßgeblichen Grundrechte und Interessen vorgenommen, die auch künftig beibehalten werden sollte.[200] Wenn hierbei eine lebende Person betroffen ist, kann das Archivgut nur mit ihrer Einwilligung zugänglich gemacht werden. In diesem Fall bestehen auch keine weitergehenden Einsichtsrechte und damit Recherchemöglichkeiten der Presse. Hingegen sieht das Archivgesetz des Bundes für diese Fälle eine gewisse Öffnung durch eine mögliche Verkürzung der Schutzfristen vor.[201] Die Voraussetzungen einer entsprechenden Öffnungsklausel im Archivgesetz wären genau zu bestimmen, um die Zahl der Anwendungsfälle zu begrenzen.

199 § 8 ArchGB
200 § 8 Abs. 3 ArchGB
201 § 5 Abs. 5 Satz 3 und 4 BArchG

Das Archivgesetz sieht außerdem vor, dass die Nutzung zu versagen ist, soweit Grund zu der Annahme besteht, dass das Wohl der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet würde.[202] Es ist klarzustellen, dass hieraus nicht geschlossen werden kann, dass Einsicht in die ehemaligen Akten des Verfassungsschutzes nur mit Zustimmung des Verfassungsschutzes erteilt werden kann. Über die Offenlegung von Archivmaterial entscheidet allein das Landesarchiv.

Auch die Nutzung von Patientendaten wirft wegen der ärztlichen Schweigepflicht[203] weitergehende Schwierigkeiten auf, die der Gesetzgeber im Archiv- und Krankenhausrecht klarstellen sollte.[204]

Nicht zuletzt besteht ein Widerspruch zum Informationsfreiheitsrecht, der durch eine Gesetzesänderung gelöst werden sollte. Aufgrund der Sperrfristen des Archivrechts müssen nach dem Informationsfreiheitsgesetz frei zugängliche Akten der Verwaltung nach Abgabe an das Archiv geheim gehalten werden.[205] Um diesen Widerspruch zu lösen, sollte eine Regelung vergleichbar der des Bundesarchivgesetzes aufgenommen werden.[206]

Die datenschutzrechtlichen Bestimmungen des Berliner Archivgesetzes, die ursprünglich Modellcharakter hatten, sollten jetzt grundlegend neu gefasst werden, um den veränderten rechtlichen, sozialen und technischen Gegebenheiten Rechnung zu tragen und die beschriebenen praktischen Probleme zu lösen. Dabei sollte Berlin nicht auf den Bundesgesetzgeber warten, sondern wie 1993 eine Vorreiterrolle übernehmen.

202 § 8 Abs. 9 Satz 1 Nr. 1 ArchGB
203 § 8 Abs. 9 Satz 1 Nr. 5 ArchGB
204 Vgl. JB 2008, 9.1
205 Vgl. Entschließung der Informationsfreiheitsbeauftragten vom 26. März 2003: Gleiche Transparenz in Verwaltung und Archiven
206 Nach § 5 Abs. 4 BArchG gelten die Schutzfristen des § 5 Abs. 1 – 3 BArchG nicht für Archivgut, soweit es vor der Übergabe bereits einem Informationszugang nach dem Informationsfreiheitsgesetz offen gestanden hat.

8.1.6 Einsatz von RFID-Technik zum Erhalt ehrenamtlich betriebener Bibliotheken

2008 haben wir von der Planung berichtet, die Medien in den öffentlichen Bibliotheken des Landes Berlin mithilfe von RFID-Technik zu verwalten.[207] Dies soll auch als Lösung für die ehrenamtlich betriebenen Bibliotheken dienen. Die Zugriffsmöglichkeiten der ehrenamtlich Beschäftigten auf die Daten der Nutzenden sind dadurch – dem Datenschutzrecht entsprechend – auszuschließen.

Die RFID-Technik ermöglicht eine Objektidentifikation mithilfe von Funkwellen. Die Daten eines mit einem RFID-Chip ausgestatteten Objekts können mit einem Lesegerät berührungslos und ohne Sichtkontakt gelesen und gespeichert werden.[208] Dieses Verfahren kann z.B. zur Diebstahlsicherung genutzt werden, wenn ein Lesegerät am Ausgang einer Bibliothek überprüft, ob ein mit einem RFID-Chip bestücktes Medium bereits verbucht ist. Der RFID-Chip enthält keine Daten über Personen, die das jeweilige Medium (Buch, DVD etc.) gegenwärtig nutzen oder früher genutzt haben. Dennoch besteht ein Datenschutzrisiko dann, wenn unbefugte Dritte die Daten eines RFID-Chips auslesen können, um das Leseverhalten von Nutzenden zu studieren, die das Medium mit sich führen. Der Verbund öffentlicher Bibliotheken Berlin (VÖBB) hat in seinem Sicherheitskonzept dieses und andere Risiken beschrieben und Sicherheitsmaßnahmen ergriffen, die einen angemessenen und wirksamen Schutz des Systems gewährleisten. Wir haben die Erstellung dieses Konzepts beratend begleitet.

In allen öffentlichen Bibliotheken Berlins sollen RFID-Selbstverbuchungsstationen eingesetzt werden. Mitte des Jahres sind die ersten Selbstverbuchungsstationen in Betrieb gegangen. An diesen Stationen können sich die Bibliotheksnutzenden zunächst registrieren, Medien entleihen und zurückgeben sowie ggf. anfallende Gebühren mittels EC-Karte bezahlen.

207 JB 2008, 1.2.3
208 Vgl. JB 2004, 3.4

Die Bibliotheksbeschäftigten werden aber auch weiterhin die Nutzenden bei der Ausleihe unterstützen. In den beiden Bibliotheken, die von ehrenamtlich Beschäftigten betrieben werden[209], soll die Entleihe, Rückgabe und Zahlung von Gebühren hingegen ausschließlich mithilfe der Selbstverbuchungsautomaten möglich sein. Dadurch müssen die dort Beschäftigten, die nicht zum Datenumgang berechtigt sind, keinen Zugang zu den Daten der Nutzenden haben.[210] Entsprechend werden dort die Datenzugriffsberechtigungen vollständig entfallen, sobald alle Funktionen der Selbstverbuchungsautomaten zur Verfügung stehen. Bis dahin besteht die auch bislang schon betriebene Übergangslösung fort, bei der der Datenzugriff der ehrenamtlich Beschäftigten durch die dienstrechtliche Aufsicht begrenzt wird.

Im Laufe des Jahres 2012 sollen die Verbuchungsvorgänge in den ehrenamtlich geführten Bibliotheken ausschließlich mithilfe der RFID-Selbstverbuchungsanlagen durchgeführt werden können. Das dafür erstellte Informationssicherheitskonzept erfüllt die datenschutzrechtlichen Anforderungen. Mithilfe der RFID-Systeme ist eine Lösung gefunden worden, die die anerkennenswerte ehrenamtliche Mitarbeit ermöglicht und gleichzeitig die Daten der Nutzenden vor unberechtigtem Zugriff schützt.

209 Thomas-Dehler-Bibliothek in Tempelhof-Schöneberg und Kurt-Tucholsky-Bibliothek in Pankow

210 Vgl. JB 2009, 8.1

8.2 Schule

8.2.1 Umsetzung des Bildungs- und Teilhabepakets in Berlin

Unter dem Begriff „Bildungs- und Teilhabepaket“ (BuT) werden neuerdings bestimmte Sozialleistungen zusammengefasst. Im Einzelnen handelt es sich um sieben unterschiedliche Leistungen, und zwar um Tagesausflüge in Schulen und Kindertagesstätten (Kita), Mittagsverpflegung in diesen Einrichtungen und in Horten, Lernförderung, Klassenfahrten, Teilhabe am gesellschaftlichen Leben, Schülerbeförderung und Ausstattung mit Schulmaterial. Anspruchsberechtigt sind Kinder aus Familien, die Arbeitslosengeld II, Sozialgeld, Sozialhilfe, Kinderzuschlag, Wohngeld oder Leistungen nach dem Asylbewerberleistungsgesetz bekommen. Im Zusammenhang mit der Umsetzung des BuT sind § 29 Sozialgesetzbuch Zweites Buch (SGB II)[211] und § 34 Sozialgesetzbuch Zwölftes Buch (SGB XII)[212] geändert worden. Bei beiden Gesetzen handelt es sich um Bundesgesetze. In Berlin wirken sich diese Gesetzesänderungen u. a. derart aus, dass das zwischen uns und der Senatsverwaltung für Integration, Arbeit und Soziales vereinbarte datenschutzkonforme Kostenübernahmeverfahren für Klassenfahrten hinfällig geworden ist. Zudem werden Stellen, die keine Sozialleistungsträger sind, in die Gewährung und Abrechnung der Leistungen aus dem BuT mit einbezogen.

Umsetzung in Schulen, Schulämtern und Schulaufsichtsbehörden

2010 haben wir berichtet, dass die Senatsverwaltung für Integration, Arbeit und Soziales, nachdem wir einen datenschutzrechtlichen Mangel festgestellt hatten, das Kostenübernahmeverfahren für Klassenfahrten durch die Berliner Jobcenter modifiziert hat. [213] Bei der Beantragung der Übernahme von Klassenfahrtkosten sollten die Eltern zukünftig in der Wahl der Mittel zur Erbringung der

211 Vgl. § 29 Abs. 1 Satz 1 SGB II
212 Vgl. § 34 a Abs. 2 Satz 1 SGB XII
213 JB 2010, 8.1.1

vom Jobcenter benötigten Nachweise frei und nicht mehr an die Verwendung eines von der Schule auszufüllenden Vordrucks gebunden sein. Eine wesentliche Änderung war zudem, dass der Geldbetrag je nach gewählter Verfahrensvariante künftig entweder vom Jobcenter oder von den Eltern selbst auf das Konto der verantwortlichen Lehrkraft überwiesen werden konnte.

Durch die Änderungen im SGB II und SGB XII ist diese datenschutzkonforme Verfahrensgestaltung nicht mehr umsetzbar. Die neuen Regelungen legen fest, dass die Leistungen für Bildung und Teilhabe, d. h. auch die Kostenübernahme für Klassenfahrten, durch Sach- und Dienstleistungen und demzufolge nicht durch die Auszahlung entsprechender Geldbeträge zu erbringen sind. Die Überweisung eines Geldbetrags vom zuständigen Leistungsträger auf das Konto der Leistungsempfängerinnen und -empfänger, damit diese den Betrag selbst an die verantwortliche Lehrkraft überweisen können, ist somit ausgeschlossen. Die Schule erhält den Betrag direkt vom zuständigen Leistungsträger und erfährt dadurch in jedem Fall vom Leistungsbezug der Eltern. Auf diese Weise wird das Recht der Eltern, selbst über die Preisgabe ihrer Sozialdaten zu entscheiden, eingeschränkt. Diese Entscheidungsfreiheit ist ein wichtiger Bestandteil des Grundrechts auf informationelle Selbstbestimmung.

Darüber hinaus führen die neuen bundesrechtlichen Regelungen in Berlin dazu, dass im Rahmen der Gewährung und Abrechnung von Leistungen aus dem BuT sowohl in den Schulen als auch in der Schulaufsichtsbehörde und den Schulämtern personenbezogene Daten der leistungsberechtigten Schülerinnen und Schüler verarbeitet werden. Auf diese Weise werden Stellen, die keine Leistungsträger im Sinne des Sozialgesetzbuches sind, in die Verarbeitung der Sozialstatusdaten der Schülerinnen und Schüler einbezogen. Für diese Datenverarbeitung gab es in Berlin zunächst keine Rechtsgrundlage. Nach intensiven Gesprächen mit der Senatsverwaltung für Bildung, Wissenschaft und Forschung konnten wir immerhin erreichen, dass das Berliner Schulgesetz um eine entsprechende Datenverarbeitungsbefugnis ergänzt wurde. [214]

Allerdings bleibt es dabei, dass nach den Grundsätzen der Datenvermeidung und Datensparsamkeit gewährleistet werden muss, dass die Datensätze einem möglichst kleinen Personenkreis zugänglich sind. Dies ist nach der derzeit für

214 § 64 Abs. 6 Berliner Schulgesetz

die Umsetzung der Bildungs- und Teilhabeleistungen vorgesehenen Verfahrensgestaltung nicht der Fall. Es sind zu viele Personen in die Datenverarbeitungsschritte einbezogen, namentlich Lehrpersonal, Schulsekretariatspersonal, die Schulleitung, die Sachbearbeiterinnen und -bearbeiter in den Behörden sowie zusätzlich die privaten Leistungsanbieter. Wenn überhaupt, dann ist es für Schulen und private Leistungsanbieter vollkommen ausreichend zu wissen, ob ein Berechtigungsstatus der jeweiligen Schülerin bzw. des jeweiligen Schülers besteht. Keinesfalls benötigen Schulen und private Leistungsanbieter Detailwissen z.B. über die konkrete Art der gewährten Sozialleistung. Ein wichtiger Schritt zur Datensparsamkeit bei der Umsetzung der Gewährung von Leistungen aus dem BuT wäre z.B. die Einführung gesonderter Schulkonten für alle Berliner Schulen. Hierauf haben wir die zuständige Senatsverwaltung hingewiesen. Inwiefern unsere Anmerkungen aufgegriffen werden, bleibt abzuwarten.

Umsetzung in Kindertageseinrichtungen

Aus dem BuT werden für leistungsberechtigte Kinder in Berliner Kindertageseinrichtungen (Kita) Kosten für die Teilnahme an Kita-Ausflügen sowie an der Mittagsverpflegung finanziert. Die bundesrechtlichen Regelungen, die vorschreiben, dass die entsprechenden Leistungen durch Sach- und Dienstleistungen und nicht durch Geldleistungen erbracht werden müssen, sind auch hier nicht datenschutzgerecht. Eltern müssen nämlich gegenüber der Kita bzw. deren Trägern ihre Leistungsberechtigung nachweisen und damit ihren Leistungsbezug offenbaren. Dennoch waren die bundesrechtlichen Vorgaben landesrechtlich umzusetzen.

In Berlin erfolgt die Abrechnung der BuT-Leistungen durch die Kita gegenüber den Jugendämtern. Bei aller Kritik an dem gesamten Verfahren begrüßen wir zumindest, dass mit den Jugendämtern Sozialleistungsträger, für die die strengen Datenschutzvorschriften des Sozialgesetzbuchs gelten, mit der Abrechnung und damit der Datenverarbeitung betraut sind. Zunächst wurde ein Verfahren etabliert, das die Abrechnung mithilfe von Listen vorsah, die von den Kita zu erstellen waren und dann zum Zweck der Abrechnung an die Jugendämter weitergeleitet wurden. Wir haben die für die Umsetzung verantwortliche Senatsverwaltung für Bildung, Wissenschaft und Forschung aufgefordert, Maßnahmen zu treffen, die gewährleisten, dass die sensiblen personenbezogenen Informationen in den jeweiligen Einrichtungen vertraulich behandelt und

insbesondere verschlossen und von anderen Unterlagen getrennt aufbewahrt werden. Diese Vorgaben wurden berücksichtigt und den mit der Umsetzung des BuT befassten Stellen mitgeteilt.

Um das mit hohem bürokratischen Aufwand verbundene Verfahren für alle Beteiligten zu vereinfachen, plante die Senatsverwaltung für Bildung, Wissenschaft und Forschung bereits frühzeitig, die Abrechnung über das entsprechende **Kita-Fachverfahren ISBJ** zu realisieren, das auch für die Finanzierung der Kita-Gutscheine verwendet wird. Noch vor der parlamentarischen Sommerpause wurde die notwendige gesetzliche Verordnungsermächtigung im Kindertagesförderungsgesetz geschaffen.[215]

Im Herbst teilte uns die Senatsverwaltung für Bildung, Wissenschaft und Forschung mit, bereits vor Inkrafttreten der Änderungsverordnung zur Kindertagesförderungsverordnung die Umsetzung der BuT-Leistungen mit dem Kita-Fachverfahren ISBJ realisieren zu wollen. Damit sollte der bürokratische Aufwand bei der Gewährung der BuT-Leistungen reduziert werden. Da eine Abrechnung über das Kita-Fachverfahren ISBJ auch aus datenschutzrechtlicher Sicht Vorteile gegenüber dem manuellen Verfahren der Abrechnung über von den Kita erstellte Listen bietet und keine datenschutzrechtlichen Bedenken gegen die technische Umsetzung bestanden, haben wir von einer förmlichen Beanstandung abgesehen. Voraussetzung hierfür war allerdings die Umsetzung unserer datenschutzrechtlichen Anforderungen in der zu erlassenden Rechtsverordnung. Die Senatsverwaltung für Bildung, Wissenschaft und Forschung hat den Text der Änderungsverordnung zur Kindertagesförderungsverordnung auf der fachlichen Ebene eng mit uns abgestimmt und unsere Vorgaben umgesetzt. Der Entwurf befand sich bei Redaktionsschluss im förmlichen Mitzeichnungsverfahren.

Wir hoffen, dass die Reduzierung des bürokratischen Aufwands bei der Gewährung der BuT-Leistungen bei allen beteiligten Stellen die Akzeptanz erhöhen wird. Es bleibt abzuwarten, ob eine datenschutzgerechte Umsetzung des Bildungs- und Teilhabepakets gelingen wird.

215 § 26 Abs. 3 Kindertagesförderungsgesetz

8.2.2 Transparente Schulinspektionen und Leistungschecks für Pädagogen

Im Frühjahr stellte der Senator für Bildung, Wissenschaft und Forschung sein „Qualitätspaket für Schule und Kita" vor. Das Paket sah u. a. die Veröffentlichung der Schulinspektionsberichte vor. Außerdem sollten Lehrkräfte ihren Unterricht regelmäßig von den Schülerinnen und Schülern unter Benutzung des Selbstevaluationsportals evaluieren (bewerten) lassen, das das Institut für Schulqualität Berlin-Brandenburg anbietet. Der rechtliche Rahmen für diese Maßnahmen sollte durch eine „Verordnung über schulische Qualitätssicherung und Evaluation"[216] geschaffen werden.

Auf Nachfrage wurde uns der Entwurf der Verordnung übersandt. Begleitend dazu teilte uns die Senatsverwaltung für Bildung, Wissenschaft und Forschung mit, dass sie ab dem nächsten Schuljahr die generelle Veröffentlichung aller Schulinspektionsberichte beabsichtige. Vorgesehen sei jedoch keine Veröffentlichung der Berichte in der Vollfassung mit allen Detailbewertungen, sondern eine Zusammenfassung. Der uns vorgelegte Entwurf der Verordnung enthielt dazu lediglich die Bestimmung, dass die Schulaufsichtsbehörde die Schulinspektionsberichte in geeigneter Form veröffentlichen kann[217]. Durch den Wortlaut der Regelung wurde der Eindruck vermittelt, dass die Senatsverwaltung sich vorbehält, lediglich die Schulinspektionsberichte der Schulen zu veröffentlichen, in denen sich die Schulkonferenz mehrheitlich gegen eine Veröffentlichung ausgesprochen hat. Die beabsichtigte Veröffentlichung aller Schulinspektionsberichte (in zusammengefasster Form) ließ sich daraus nicht eindeutig ableiten. Wir haben daher empfohlen, den Text der Verordnung zur Klarstellung zu ändern. Es sollte deutlich gemacht werden, dass zukünftig alle Schulinspektionsberichte – unabhängig von der Entscheidung in der jeweiligen Schulkonferenz – nach einheitlichen Kriterien in geeigneter Form durch die Senatsverwaltung veröffentlicht werden. Bewertungen über Schulleiterinnen und Schulleiter dürfen dabei nur im unerlässlichen Umfang in die Berichte eingehen und veröffentlicht werden.

216 SchulQualSiEvalVO
217 Vgl. § 5 Abs. 3 Satz 5 des Entwurfs

Unsere Empfehlungen wurden umgesetzt. Zunächst wurde klargestellt, dass personenbezogene Daten der Schulleiterin oder des Schulleiters bei der Erstellung des Schulinspektionsberichts nur verarbeitet werden dürfen, soweit dies nach Sinn und Zweck des Berichts zwingend erforderlich ist.[218] Des Weiteren wurde eine neue Regelung in die Verordnung aufgenommen, die eindeutig festlegt, dass die Schulaufsichtsbehörde eine Zusammenfassung der wesentlichen Ergebnisse der Schulinspektionsberichte veröffentlicht.[219]

Auch unsere Empfehlungen zur Nutzung des Selbstevaluationsportals beim Institut für Schulqualität Berlin-Brandenburg wurden aufgegriffen. So wurde in der Verordnung sichergestellt, dass nur die betroffenen Lehrkräfte einen Zugang zu den individualisierten Ergebnissen der Evaluation erhalten.[220] Die Ergebnisse der Evaluation dürfen auch nicht an der Schule dokumentiert oder aufbewahrt werden.[221] Eine Nutzung der Evaluationsergebnisse für wissenschaftliche Zwecke ist nur in anonymisierter Form zulässig.[222]

Durch die nun normenklaren Regelungen in der Verordnung über schulische Qualitätssicherung und Evaluation konnte nicht nur für mehr Transparenz in Bezug auf Schulinspektionen gesorgt, sondern auch das Recht auf informationelle Selbstbestimmung der Lehrkräfte bei der Nutzung des Selbstevaluationsportals zur Bewertung ihrer Unterrichtsleistung ausreichend gesichert werden.

218 § 5 Abs. 1 Satz 3 SchulQualSiEvalVO
219 § 5 Abs. 4 Satz 1 SchulQualSiEvalVO
220 § 6 Abs. 3 Satz 1 SchulQualSiEvalVO
221 § 6 Abs. 4 SchulQualSiEvalVO
222 § 6 Abs. 2 Satz 3 SchulQualSiEvalVO

8.2.3 Das abgelehnte Kind – Einsicht in die Sprachtestunterlagen

Eine Lehrkraft informierte uns über folgenden Sachverhalt: Zum Nachweis einer ausreichenden Sprachkompetenz müssen Kinder, die die Aufnahme an einer zweisprachigen (Europa-)Grundschule beantragt haben, einen standardisierten Sprachtest machen. Eltern, deren Kinder diesen Test nicht bestehen, versuchen zunehmend, die Zulassung der Kinder auf dem Rechtsweg zu erstreiten. Zu diesem Zweck beantragen und erhalten die beauftragten Rechtsanwälte beim zuständigen Schulamt grundsätzlich Einsicht in die Testergebnisse aller Kinder, die an dem Test teilgenommen haben. Die Ergebnisse der Sprachprüfung werden in den Aufnahmeunterlagen der einzelnen Kinder dokumentiert. Durch die Einsichtnahme in diese Unterlagen erhalten die Rechtsanwälte somit auch Kenntnis über sämtliche personenbezogene Daten der Kinder aus dem Aufnahmeverfahren (u. a. Name, Geburtsdatum und Geburtsort) sowie die Namen der an dem Testverfahren beteiligten Lehrkräfte. Das zuständige Schulamt bestätigte uns, dass den Rechtsanwälten als Verfahrensbevollmächtigten regelmäßig die umfassende Einsichtnahme in den Generalvorgang zu jedem Kind gewährt wird, das an dem Test teilgenommen hat.

Während des Verwaltungsverfahrens haben die an dem Verfahren Beteiligten einen Anspruch auf Einsicht in die das Verfahren betreffenden schriftlichen Unterlagen.[223] Das von der Schulaufnahme ausgeschlossene Kind bzw. dessen Eltern sind als die Adressaten eines belastenden Verwaltungsakts Beteiligte an dem Verfahren.[224] Der von ihnen bevollmächtigte Rechtsanwalt hat daher grundsätzlich ein Recht auf Akteneinsicht.

Durch die Einsichtnahme in den Generalvorgang wird dem bevollmächtigten Rechtsanwalt u. a. der Name und damit die Identität der Lehrkraft offenbart, die den Sprachtest durchgeführt und bewertet hat. Dem zu schützenden Geheimhaltungsinteresse der Lehrkraft, abgeleitet aus ihrem Grundrecht auf informationelle Selbstbestimmung, steht hier das Recht auf Akteneinsicht

223 Vgl. § 4 a Abs. 1 VwVfGBln
224 Vgl. § 13 VwVfG

der Verfahrensbeteiligten entgegen. In Anbetracht des weiten prüfungsrechtlichen Beurteilungsspielraumes sind an die Einwände gegen eine Prüfungsbewertung sehr hohe Anforderungen zu stellen. Durch eine Beschränkung ihres Akteneinsichtsrechts würden die Beteiligten zusätzlich in ihren Wissens- und Verteidigungsmöglichkeiten eingegrenzt. Die Kenntnis des Namens der prüfenden Person kann im Übrigen die erforderliche Voraussetzung für die wirksame Geltendmachung der Rechte im Widerspruchsverfahren sein. Ohne diese Angaben wäre eine etwaige Überprüfung einer möglichen Befangenheit oder Voreingenommenheit der Prüferin oder des Prüfers stets ausgeschlossen. Bei der Durchführung der Sprachtests ist das Gebot der Chancengleichheit einzuhalten. Das Recht auf Akteneinsicht der oder des Verfahrensbeteiligten schafft hier die erforderliche Transparenz. Sie oder er kann so z.B. feststellen, ob von den Prüfkräften vergleichbare Bewertungsstandards bzw. Maßstäbe angewandt wurden. Daher sind grundsätzlich alle Unterlagen zu den Sprachtests, die im Zuge der Aufnahmeprüfung an der Grundschule angefertigt wurden, von der Reichweite des gesetzlichen Akteneinsichtsrechts umfasst.

Allerdings stehen der umfassenden Akteneinsicht der Verfahrensbeteiligten die berechtigten Interessen der anderen am Test teilnehmenden Kinder an der Geheimhaltung ihrer Daten aus dem Aufnahmeverfahren an der Schule entgegen. Diese Daten (z.B. Name, Vorname, Geburtsdatum, Adresse, gesundheitliche Einschränkungen, Förderbedarf) sind für die Verfolgung der Rechtsinteressen der abgelehnten Kinder grundsätzlich nicht erforderlich. Im Rahmen der gebotenen Abwägung der kollidierenden rechtlichen Interessen ist daher eine teilweise Einschränkung der Akteneinsicht geboten (z.B. durch Schwärzung der personenbezogenen Daten der anderen Kinder).

Vor der Einsichtnahme der Aufnahmeunterlagen (einschließlich Sprachtest) aller am Test teilnehmenden Kinder durch die Anwälte der abgelehnten Kinder sind die personenbezogenen Daten der Kinder (z. B. Name, Vorname, Geburtsdatum, Adresse) unkenntlich zu machen.

9. Wirtschaft

9.1. Banken und Versicherungen

9.1.1 Schlimmer geht's nimmer

Aus der Praxis

Eine Bankkundin wollte ihr Konto auflösen und bat deshalb darum, ihr ein Formular zur Kontolöschung per E-Mail zuzuleiten. Sie wunderte sich nicht schlecht, als ihr anstelle des Formulars eine Datei mit dem Namen „Kontoschließung" zugeschickt wurde, die die Namen und Kontonummern von fast 700 Kunden der Bank sowie interne Verarbeitungsvermerke enthielt. Diese dokumentierten Informationen wie Nachlassfall, Konto wiederbelebt, Karten angefordert. Die Daten stammten aus 2008 und 2009.

Ein Bankmitarbeiter hatte versehentlich anstelle des gewünschten Formulars die Excel-Datei mit den Kundendaten als Anlage zu seinem Schreiben verschickt. Dabei hatte er die Weisung seiner Bank, jede verschickte Anlage noch einmal zu kontrollieren, nicht beachtet. Der Name der Excel-Datei „Kontoschließung" führte bei ihm zu dem Irrtum, dass es sich um das gewünschte Formular handelte.

Die Bank hätte dem Mitarbeiter aber gar nicht die „Gelegenheit" geben dürfen, einen derartigen Fehler zu begehen. Da die Daten aus 2008 und 2009 stammten, hätten sie – da sie für das operative Geschäft nicht mehr erforderlich waren – gelöscht oder gesperrt werden müssen. Die Bank will nun sicherstellen, dass die Kontoschließungsdatei innerhalb von drei Monaten nach ihrer Erstellung automatisch gelöscht wird. Das Datensicherungskonzept der Bank wäre aber auch dann zu kritisieren gewesen, wenn es sich um eine aktuelle Datei gehandelt hätte. Dem Kundenbetreuer ist ein lesender und evtl. schreibender Zugriff auf die für die Kundenbetreuung erforderlichen Daten zu gewähren; diese sind aber so abzuspeichern, dass er nicht in der Lage ist, ganze Dateien zu übermitteln.

Die Bank hat den Vorfall zum Anlass genommen, ihr Lösch- und Sperrkonzept, die Zugriffsrechte und die Schulung der Beschäftigten zu verbessern. Auf Bitte der Bank hat die Empfängerin der Datei glaubhaft bestätigt, dass sie alle erhaltenen Daten gelöscht hat.

Durch aufgabenbezogene Zugriffsberechtigungen und ein Lösch- und Sperrkonzept lässt sich verhindern, dass Flüchtigkeitsfehler von Mitarbeiterinnen und Mitarbeitern gravierende Auswirkungen haben.

9.1.2 Eine Bank will zu viel wissen

Aus der Praxis

Zwei Bürger beschwerten sich über eine Online-Bank, die zu viele Daten abfrage: Bei Kreditantragstellung verlange die Bank, dass die Kreditinteressentinnen und -interessenten die Kontoauszüge der letzten sechs Wochen vorlegen. Dies sei erforderlich, um die Kreditwürdigkeit der Betroffenen zu überprüfen. Dieselbe Bank forderte von einem Kunden, der sein Konto kündigen wollte, die Mitteilung seiner neuen Bankverbindung, anderenfalls würde man seine Kündigung nicht akzeptieren.

Kreditinstitute sind verpflichtet, vor Abschluss eines Verbraucherdarlehensvertrages u. a. durch Auskünfte des Verbrauchers dessen Kreditwürdigkeit zu prüfen.[225] Bei einem Kreditantrag sind sie grundsätzlich berechtigt, Kontoauszugsdaten anzufordern. Diese können zahlreiche – teils auch sensitive – Daten enthalten wie die Begleichung von Arzt- und Psychotherapeutenrechnungen, die Bezahlung einer Rechnung von Beate Uhse, einer Geldstrafe oder die Zahlung der Mitgliedsbeiträge für eine politische Partei. Diese und ähnliche Daten müssen auch nicht allein die Kreditnehmenden betreffen; es kann sich auch um personenbezogene Daten etwa der Ehefrau des Kreditnehmers (Gemeinschaftskonto) handeln. Viele der Kontobewegungen werden keine Relevanz für die Frage enthalten, ob dem Kreditantrag entsprochen und zu welchen Konditionen der Kredit gewährt wird. Die Anforderung von Kontoauszügen ist nur rechtmäßig, wenn die Betroffenen das Recht haben, nicht kreditrele-

225 Vgl. § 18 Abs. 2 Kreditwesengesetz (KWG)

vante Informationen zu schwärzen, um nicht ein Übermaß an Daten zu erheben. Die Banken sind verpflichtet, die Kunden auf die Schwärzungsmöglichkeit hinzuweisen. Die Online-Bank hat uns mitgeteilt, künftig entsprechend unseren Vorgaben zu verfahren.

Bei der Abwicklung eines Bankkontos ist es für die Bank hilfreich, die neue Bankverbindung von den Betroffenen zu erhalten, um leichter Guthaben- oder Sollsalden zu verrechnen. Trotzdem bleibt die Mitteilung des Abrechnungskontos freiwillig, die Nennung dieses Datums darf nicht zur Voraussetzung für eine Kontokündigung gemacht werden. Auch hier hat die Bank zugesagt, unsere Vorgaben zu beachten.

Häufig erheben Banken und andere verantwortliche Stellen zu leichtfertig Daten, für die keine Erforderlichkeit besteht.

9.1.3 Ungenügender Schutz von Kontodaten

Bei den SB-Terminals der Sparkassen haben EC-Karteninhaberinnen und -inhaber die Möglichkeit, ohne PIN-Eingabe unter dem Punkt „Empfängerauswahl“ Einsicht in die zehn zuletzt getätigten Überweisungen zu nehmen. Zu den angezeigten Daten gehören Bankleitzahl, Kontonummer und der Empfängername. Bestimmte personenbezogene Daten sind auch bei den Funktionen „Dauerauftrag“ und „Umbuchung“ sichtbar. Ein Bankkunde beschwerte sich darüber, dass unberechtigte Besitzer von EC-Karten auf personenbezogene Daten zugreifen können.

Wenn eine EC-Karte verloren geht, hat die Karteninhaberin bzw. der Karteninhaber die Pflicht, die Karte unverzüglich sperren zu lassen, u. a. um ein Ausspähen von Daten zu verhindern. Gleichzeitig werden sie dafür Sorge tragen, dass die EC-Karte bestmöglich vor Diebstahl geschützt ist. Bei der Mehrzahl der Banken erhält man Kontoauszüge ohne PIN-Eingabe. Dies erscheint vertretbar, da Kontoauszüge nur die Bankverbindungsdaten der Karteninhaberin bzw. des Karteninhabers enthalten, nicht jedoch die der überweisenden Person. Hier können die Karteninhaberinnen und -inhaber durch Selbstdaten-

schutz dazu beitragen, dass die eigenen Daten nicht Unberechtigten zugänglich gemacht werden. Die nicht PIN-geschützte Speicherung von Überweisungsdaten führt aber dazu, dass sensitive Kontodaten unrechtmäßig Dritten zur Kenntnis gelangen können, ohne dass die Betroffenen dies bemerken oder verhindern können. Ein Selbstdatenschutz ist hier nicht möglich. Wir haben den betroffenen Bankenverband aufgefordert, seine Mitglieder auf die Pflicht hinzuweisen, den Zugang zu Überweisungsdaten nur nach PIN-Abfrage zu ermöglichen.

Eine PIN-Eingabe ist erforderlich, sobald am Kundenterminal nicht nur der Kontoauszug gedruckt wird, sondern darüber hinausgehende Informationen zur Verfügung gestellt werden, etwa Überweisungsdaten.

9.1.4 Positive Entwicklung in der Versicherungswirtschaft

Aus der Praxis

„Ich willige ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer zur Beurteilung des Risikos oder zur Abwicklung der Rückversicherung sowie zur Beurteilung des Risikos und der Ansprüche an andere Versicherer und/oder an den Gesamtverband der Deutschen Versicherungswirtschaft e. V. zur Weitergabe dieser Daten an andere Versicherer übermittelt. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Vertrages sowie für entsprechende Prüfungen bei anderweitig beantragten (Versicherungs-)Verträgen und bei künftigen Anträgen."

Die Aufsichtsbehörden haben seit 2005 in Verhandlungen mit der Versicherungswirtschaft gefordert, dass diese Einwilligungsklausel nicht mehr verwendet wird, da die oder der Versicherungsnehmende bei Unterzeichnung der Erklärung nicht überblicken kann, welche Konsequenzen die Einwilligung hat. Die Klausel ist deshalb so unbestimmt, weil sie für alle Versicherungsverträge mit Ausnahme der privaten Krankenversicherung Anwendung findet. Auch die Freiwilligkeit der Einwilligungserklärung erscheint mehr als zweifelhaft. Teils wurde der Abschluss einer Versicherung bei fehlender Unterschrift abgelehnt,

teils erfolgten die in der Einwilligungserklärung genannten Datenverarbeitungen ohne Einwilligung unter Berufung auf gesetzliche Regelungen.

Die Versicherungswirtschaft hat sich in den Verhandlungen 2011 bereiterklärt, die Klausel nach möglichst kurzer Übergangszeit, spätestens jedoch nach dem 31. Dezember 2012 nicht mehr zu verwenden. Grundsätzlich wird sich die Versicherungswirtschaft auf Datenerhebungen, -verarbeitungen und -nutzungen beschränken, für die das BDSG eine Rechtsgrundlage enthält. Anstelle der zweifelhaften Einwilligungserklärung wird sie dafür sorgen, dass die Datenverarbeitung für die Versicherten transparent ist. Allerdings ist bei der Erhebung und Verwendung von Gesundheitsdaten in bestimmtem Umfang weiterhin eine Einwilligungserklärung, teilweise auch eine Schweigepflichtentbindungserklärung erforderlich. Hierzu hat die Versicherungswirtschaft in Zusammenarbeit mit den Aufsichtsbehörden neue Einwilligungs- und Schweigepflichtentbindungsklauseln entwickelt, die nach dem Baustein-System verwendet werden, soweit hierzu im Einzelfall eine Erforderlichkeit besteht.

2006 haben wir im Einzelnen dargestellt, dass das Hinweis- und Informationssystem der Versicherungswirtschaft gegen das BDSG verstößt und durch ein datenschutzkonformes Auskunfteisystem ersetzt werden sollte.[226] Nach längeren Verhandlungen hat die Versicherungswirtschaft nun im April unsere Forderung erfüllt. Datenübermittlungen von und zu der beauftragten Auskunftei, die informa Insurance Risk and Fraud Prevention GmbH, erfolgen nur, wenn das BDSG dies erlaubt. Anders als im alten Hinweis- und Informationssystem stellt die jetzige Warndatei der Versicherungswirtschaft kein „schwarzes Loch" mehr dar; insbesondere werden nunmehr die Benachrichtigungs-, Auskunfts- und Löschpflichten eingehalten.

Die Versicherungswirtschaft beabsichtigt außerdem, 2012 als erste Branche Verhaltensregeln für den Umgang mit personenbezogenen Daten (Code of Conduct) vorzulegen. Diese werden vom Berliner Beauftragten für Datenschutz und Informationsfreiheit auf die Vereinbarkeit mit dem geltenden Datenschutzrecht überprüft werden.[227] Die Verhaltensregeln sollen die Regelungen des

226 JB 2006, 2.3
227 § 38a BDSG

BDSG für die Versicherungsbranche konkretisieren und ergänzen und damit die Rechtssicherheit erhöhen.

Die langjährigen Verhandlungen mit der Versicherungswirtschaft werden den Datenschutzstandard in dieser Branche deutlich erhöhen.

9.2 Werbeschreiben, Abofallen

9.2.1 Ein überraschendes Schreiben

Aus der Praxis

Viele Bürgerinnen und Bürger beschwerten sich über ein Medienunternehmen, das Bestätigungsschreiben über eine angeblich erteilte telefonische Einwilligung in Werbung per Telefon, E-Mail oder SMS übersandte. Die Betroffenen bestritten eine solche telefonische Einwilligung. Das Unternehmen behauptete hingegen, die telefonischen Einwilligungen seien im Sommer 2010 erteilt worden. Die Bestätigungsschreiben habe es allerdings erst im Januar 2011 versandt.

Soweit eine Einwilligung in die Verarbeitung und Nutzung von Daten zu Werbezwecken nicht schriftlich, sondern telefonisch erteilt wird, muss das Unternehmen den Betroffenen den Inhalt der Einwilligung schriftlich bestätigen.[228] Die Betroffenen sollen dadurch in die Lage versetzt werden, die Reichweite ihrer Einwilligung abzuschätzen. Die Versendung dieses Bestätigungsschreibens hat unverzüglich zu erfolgen.

Vorliegend ließ sich aufgrund der erst nach einem halben Jahr erfolgten Zusendung des Bestätigungsschreibens nicht mehr sicher aufklären, ob die Betroffenen die Telefongespräche vergessen oder die für das Unternehmen tätigen Call-Center falsche Eintragungen vorgenommen hatten. Unabhängig davon, welcher der beiden Sachverhalte zugrunde gelegt wird, hat das Unternehmen gegen Datenschutzrecht verstoßen: Entweder haben die Betroffenen nicht ein-

228 § 28 Abs. 3 a Satz 1 BDSG

gewilligt, sodass auch kein Bestätigungsschreiben erforderlich war und Werbung per SMS, Telefon oder E-Mail nicht durchgeführt werden durfte, oder das Bestätigungsschreiben erfolgte verspätet. Wir haben das Unternehmen aufgefordert, künftig Bestätigungsschreiben unverzüglich zu versenden und das Verfahren zu den telefonischen Einwilligungen so zu gestalten, dass Falscheintragungen in der Datenbank ausgeschlossen werden.

Eine Einwilligung in die Verarbeitung und Nutzung von Daten zu Werbezwecken kann – soweit die Vorgaben des Gesetzes gegen den unlauteren Wettbewerb beachtet werden[229] – auch telefonisch erteilt werden. Das Unternehmen muss dann aber den Betroffenen den Inhalt der Einwilligung unverzüglich schriftlich bestätigen.

9.2.2 Abgezockt – Kostenfallen im Internet

Viele Bürgerinnen und Bürger beschwerten sich über die Vorgehensweise eines Inkassounternehmens, nachdem sie im Internet in eine sog. Kostenfalle geraten waren. Bei solchen scheinbar kostenlosen Angeboten setzen Firmen durch eine geschickte Gestaltung des Online-Angebots auf die Unvorsichtigkeit der Nutzerinnen und Nutzer. Über eine Datenerhebungsmaske werden personenbezogene Daten wie Name, Anschrift, E-Mail-Adresse und Geburtsdatum abgefragt. An unauffälliger Stelle weisen die Firmen mit einem oft schwer lesbaren Text darauf hin, dass es sich um ein kostenpflichtiges Angebot handelt. Selbst wenn die Betroffenen das Zustandekommen eines Vertrages bestreiten, schalten diese Firmen regelmäßig ohne Beachtung dieser Einwände das Inkassounternehmen ein. Die durch dieses Inkassounternehmen versandten Mahnungen enthalten auch Drohungen wie den Hinweis auf einen Eintrag bei einer Auskunftei. Die verunsicherten Betroffenen wenden sich dann an uns mit der Bitte, die Löschung ihrer Daten bei diesem Inkassounternehmen durchzusetzen, um den Versand weiterer Mahnungen und Gerichtsverfahren unmöglich zu machen.

229 § 7 Abs. 2 Nr. 2 UWG

Die Löschung der Daten bei dem Inkassounternehmen bzw. (wegen etwaiger Aufbewahrungspflichten) die Entfernung der Daten aus dem operativen Bereich ist abhängig von der Frage, ob bei diesen Kostenfallen ein Vertrag zustande gekommen ist. Letztlich muss diese Frage von den Zivilgerichten geklärt werden. Solange eine Entscheidung dazu nicht vorliegt, können wir eine Löschung der Daten nicht durchsetzen, denn das Inkassounternehmen kann sich für die Erhebung und Speicherung der Daten auf eine Rechtsgrundlage stützen.[230] Ein berechtigtes Interesse des Unternehmens an der Datenspeicherung kann bis zur gerichtlichen Entscheidung nur dann abgelehnt werden, wenn die außergerichtliche und gerichtliche Verfolgung des Anspruchs offenbar rechtsmissbräuchlich ist. Soweit sich Bürgerinnen und Bürger an uns gewandt haben, hat das Inkassounternehmen aufgrund unseres Einschreitens die Datensätze für eine Weitergabe an Dritte und insbesondere Auskunfteien gesperrt.[231] Weitere Handlungsmöglichkeiten bietet das Datenschutzrecht nicht.

Um Verbraucherinnen und Verbraucher künftig besser vor Kostenfallen und unerwünschten Vertragsabschlüssen im Internet zu schützen, hat die Bundesregierung einen Gesetzentwurf in den Deutschen Bundestag eingebracht.[232] Dieser sieht bei kostenpflichtigen Angeboten vor, dass die Verbraucherinnen und Verbraucher einen Button anklicken, der sie über die Zahlungspflicht informiert (sog. Button-Lösung). Sie sollen dann erst nach Bestätigung der Zahlungspflicht an den Vertrag gebunden sein, sodass Abo-Fallen künftig nicht mehr möglich sein werden, sofern der Entwurf verabschiedet wird.

Bis zum Inkrafttreten einer Button-Lösung sollten Nutzerinnen und Nutzer bei (angeblichen) Online-Gratisangeboten besonders misstrauisch sein, wenn umfangreiche Angaben zu persönlichen Daten auf Internetseiten abgefragt werden. Solche Seiten sollten umgehend verlassen werden.

230 § 28 Abs. 1 Satz 1 Nr. 2 BDSG
231 § 28a Abs. 1 Satz 1 Nr. 4 d) BDSG
232 BT-Drs. 17/7745

9.2.3 Merkwürdiger Zusatz auf Werbeschreiben

Viele Bürgerinnen und Bürger erhalten personalisierte Werbeschreiben von Unternehmen, zu denen sie bisher keine vertraglichen Beziehungen haben. Auf die Nachfrage, warum das Unternehmen ihre Daten speichere, erhielten sie häufig die Auskunft, dass dies nicht der Fall sei. Die Unternehmen wiesen meist zusätzlich darauf hin, dass dies im Werbeschreiben auch an dem Zusatz „verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist die X-GmbH“ deutlich werde. Die Betroffenen vermuteten einen Datenschutzverstoß und wandten sich deshalb an uns.

In diesen Fällen liegt kein Datenschutzverstoß vor. Tatsächlich hat das werbende Unternehmen niemals für dieses Werbeschreiben von einem anderen Unternehmen personenbezogene Daten erhalten. Vielmehr hat es ein anderes Unternehmen (z.B. die X-GmbH) gebeten, seine Datenbestände nach geeigneten Personen zu durchforsten. Dieses andere Unternehmen hat dann auch den Versand der Werbung unter Hinzufügung der zuvor ausgewählten Adressdatensätze übernommen. Zwischen den beteiligten Unternehmen hat kein Datenfluss stattgefunden. Dieses Vorgehen ist nach § 28 Abs. 3 Satz 5 BDSG zulässig, soweit dabei sog. Listendaten verwendet werden. Zu solchen Listendaten gehören auch der Name, der Vorname und die Anschrift. Außerdem muss in dem Werbeschreiben die verantwortliche Stelle für die Nutzung der personenbezogenen Daten genannt werden. Dies erfolgt durch den meist kleingedruckten Zusatz „Verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist … (z.B. die X-GmbH)“. Die verantwortliche Stelle speichert die personenbezogenen Daten der Betroffenen. An diese Stelle sollten die Betroffenen ihren jederzeit möglichen Widerspruch gegen Werbesendungen richten.

Nicht immer greift ein werbendes Unternehmen für personalisierte Werbung auf gespeicherte Daten in seiner Datenbank zurück. Der Versand von solchen Werbebriefen kann durch andere Unternehmen übernommen werden, die zuvor ihre eigenen Datenbanken nach geeigneten Personen durchsucht und deren Adressen dem fremden Werbeschreiben hinzugefügt haben. In diesem Fall muss in dem Werbeschreiben der Hinweis auf das andere Unternehmen durch den Zusatz „verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist…“ enthalten sein.

9.3 Datenschutzmängel bei Markt- und Meinungsforschungsinstitut

Im Rahmen der Aufsicht über Berliner Wirtschaftsunternehmen, die personenbezogene Daten verarbeiten, führen wir regelmäßig anlassunabhängige Kontrollen und Prüfbesuche durch. Dabei gilt ein besonderes Augenmerk denjenigen Unternehmen, die in großem Umfang personenbezogene Daten verarbeiten, wie Unternehmen der Markt- und Meinungsforschung. In dieser Branche ist ein hohes Datenschutzniveau besonders wichtig, da viele sensitive Daten der Bürgerinnen und Bürger erhoben und ausgewertet werden. Aufgrund ihrer wichtigen gesellschaftlichen Aufgabe werden diese Unternehmen zwar vom Gesetzgeber in vielerlei Hinsicht datenschutzrechtlich privilegiert, allerdings müssen auch diese sich an bestimmte datenschutzrechtliche Regeln halten.

Anlässlich einer angekündigten Prüfung in einem Markt- und Meinungsforschungsinstitut haben wir eine Vielzahl von gravierenden Datenschutzmängeln festgestellt. Überrascht hat uns, dass die Person, der der betriebliche Datenschutz von der Unternehmensleitung übertragen wurde, nur unzureichende Kenntnisse vom Datenschutzrecht hatte. Gesetzliche Aufgabe von betrieblichen Datenschutzbeauftragten ist es, auf die Einhaltung der gesetzlichen Bestimmung zum Datenschutz hinzuwirken.[233] Die bestellte Person konnte weder nachweisen, dass sie in dieser Hinsicht ausgebildet war, noch waren ihr auf Nachfrage die elementaren Prinzipien des Datenschutzrechts geläufig.

Daneben mussten wir einen Verstoß gegen die Meldepflicht feststellen. Unternehmen in bestimmten Branchen, die mit einer Vielzahl von personenbezogenen Daten arbeiten, sind verpflichtet, ihre Datenverarbeitungsverfahren bei uns anzumelden.[234] Dazu gehören auch die Unternehmen der Markt- und Meinungsforschung. Bei unserem Prüfbesuch wurde offensichtlich, dass die uns vorgelegte Meldung veraltet und unvollständig war. Ebenfalls ist uns aufgefallen, dass personenbezogene Daten in einem externen Rechenzentrum verarbeitet werden, ohne dass ein schriftlicher Vertrag zwischen dem Markt- und

233 § 4e Abs. 1 Satz 1 BDSG
234 § 4d BDSG

Meinungsforschungsinstitut und dem Rechenzentrum besteht, der die Rechte und Pflichten der Parteien im Hinblick auf die Datenverarbeitung regelt.

Auch war zweifelhaft, ob die Angerufenen von dem Markt- und Meinungsforschungsunternehmen ordnungsgemäß über die Datenverarbeitung belehrt werden. Als wir Einsicht in die entsprechenden Schulungsunterlagen der Interviewer nehmen wollten, wurde uns dies verweigert. Ebenfalls wurde uns weder Einblick in die Akten des betrieblichen Datenschutzes noch in die Personalakten gewährt. Dabei sind die unserer Aufsicht unterliegenden Unternehmen gesetzlich verpflichtet, diese Überprüfungsmaßnahmen zu dulden.[235] Auch im Nachgang der Prüfung verlief die Zusammenarbeit mit dem Institut äußerst unbefriedigend. So bedurfte es einer förmlichen Anordnung, um die Person abzuberufen, der von der Unternehmensleitung der betriebliche Datenschutz übertragen worden war. Unabhängig davon haben wir ein Bußgeldverfahren gegen das Unternehmen eingeleitet.

Auch Institute der Markt- und Meinungsforschung müssen den Datenschutz ernst nehmen und sich an bestimmte Regeln halten. Unsere Behörde prüft regelmäßig die Einhaltung dieser Vorschriften auch vor Ort.

9.4 Aus der Arbeit der Sanktionsstelle

Beim Umgang mit personenbezogenen Daten besteht ein hohes Missbrauchspotenzial. Immer wieder kommt es vor, dass rechtswidrig erlangte Daten geschäftsmäßig genutzt werden. Bußgeld- sowie Strafverfahren sind daher wichtige Instrumente, um Verstöße gegen Datenschutzvorschriften zu sanktionieren. Bei der Durchführung von Bußgeldverfahren sind spezielle Kenntnisse erforderlich. Diese Verfahren werden daher bei uns von einer zentralen Stelle, der Sanktionsstelle, durchgeführt. Zur weiteren Professionalisierung der Bußgeldverfahren und zum Austausch von Erfahrungen bei den Aufsichtsbehörden hat der Düsseldorfer Kreis eine Arbeitsgruppe Sanktionen eingerichtet, die von uns geleitet wird.

235 § 38 Abs. 4 Satz 4 BDSG

Wir haben 11 Bußgeld- oder Verwarnungsbescheide erlassen und Geldbußen von insgesamt 22.705 Euro festgesetzt. In acht Fällen wurden Strafanträge gestellt.

Nach dem Gesetz über Ordnungswidrigkeiten kann, wenn eine Leitungsperson die Ordnungswidrigkeit begeht, ein selbstständiger Bußgeldbescheid gegen das Unternehmen als Nebenfolge dieser Pflichtverletzung der Leitungsperson erlassen werden.[236] Bei Vorliegen der Voraussetzungen nutzen wir diese Möglichkeit.

Wenn sanktionsbewehrte Datenschutzpflichtverletzungen nicht durch eine Leitungsperson, sondern durch „einfache" Beschäftigte verwirklicht werden, kann eine Aufsichtspflichtverletzung der Leitungsperson vorliegen. Hier besteht ebenfalls die Möglichkeit, ein Bußgeld gegen das Unternehmen selbst festzusetzen.[237] Von dieser Möglichkeit haben wir im folgenden Fall Gebrauch gemacht und ein Bußgeld in fünfstelliger Höhe festgesetzt:

Aus der Praxis

Die Geschädigten schlossen zur Erstellung von Seiten im Internet Verträge mit dem betreffenden Unternehmen ab. Gleichzeitig willigten sie ein, dass dieses Unternehmen bei einer bundesweit tätigen Auskunftei Abfragen durchführen durfte. Die Abfragen führte allerdings nicht das Unternehmen selbst durch, sondern der Mutter-Konzern mit Sitz in Düsseldorf, der auch den alleinigen Zugang zu dem Konto der Auskunftei besaß. Die Beschäftigten des Unternehmens veranlassten die Übermittlung der Daten der Geschädigten an den Mutter-Konzern. Da es kein Konzernprivileg im Datenschutzrecht gibt, lag eine rechtswidrige Datenübermittlung vor. Die Datenübermittlung konnte nämlich weder auf eine Einwilligung noch auf eine Rechtsgrundlage gestützt werden. Die Geschäftsleitung unterließ es, die erforderlichen organisatorischen Maßnahmen zur Verhinderung dieser rechtswidrigen Datenübermittlung zu treffen. Es lag somit eine Aufsichtspflichtverletzung vor. Das Unternehmen hat gegen unseren Bußgeldbescheid Einspruch eingelegt, den wir zur Entscheidung an das Amtsgericht Tiergarten abgegeben haben.

236 § 30 Abs. 4 OWiG
237 § 30 Abs. 1 und 4 i.V. m. § 130 OWiG

Die Aufsichtsbehörde hat bei festgestellten Datenschutzverstößen auch die Möglichkeit, Maßnahmen zur Beseitigung anzuordnen.[238] Hiervon haben wir in zwei Fällen Gebrauch gemacht. In einem Fall haben wir eine Anordnung erlassen, um die Entfernung von personenbezogenen Daten von Richterinnen und Richtern aus dem Internet zu erreichen.[239] In einem anderen Fall haben wir verlangt, dass die Person, der von einem Markt- und Meinungsforschungsinstitut der betriebliche Datenschutz übertragen worden war, abberufen wird, weil die erforderliche Fachkunde nicht vorlag.[240] In drei weiteren Verfahren war eine Anordnung nicht mehr notwendig, weil die Unternehmen bereits nach dem Anhörungsverfahren unseren Forderungen nachgekommen sind.

Nicht immer reicht es aus, verantwortliche Stellen zu beraten, teilweise ist es auch erforderlich, die Einhaltung des Datenschutzrechts durch Zwangsmittel sicherzustellen.

238 § 38 Abs. 5 BDSG
239 Siehe 5.2
240 Siehe 9.6

10. Europäischer und internationaler Datenschutz

10.1 Europäische Union

Die Erarbeitung des neuen **europäischen Rechtsrahmens**[241] ist in der Europäischen Kommission vorangeschritten. Kern der Reformpläne ist die Überarbeitung der für den europäischen Binnenmarkt geltenden Datenschutzrichtlinie 95/46/EG. Es wird eine weitere Harmonisierung des in der EU vorhandenen nationalen Datenschutzniveaus angestrebt, was nach Auffassung der Kommission am Ehesten durch eine Verordnung erreicht werden kann. Denn im Gegensatz zur bisherigen Rechtslage müsste eine Verordnung nicht in nationales Recht umgesetzt werden, weil sie in jedem EU-Mitgliedstaat unmittelbar gilt. In welchem Verhältnis dann die nationalen Datenschutzbestimmungen wie das BDSG und die Landesdatenschutzgesetze zum Unionsrecht stehen, bleibt abzuwarten. Bis zum Ende des Berichtszeitraums lag ein offizieller Verordnungsentwurf noch nicht vor, allerdings wurde die Entwurfsfassung einer allgemeinen EU-Datenschutzverordnung „geleakt" und ins Internet gestellt.[242] Demgegenüber soll der Schutz personenbezogener Daten im Bereich der Polizei und Justiz gesondert durch eine Richtlinie geregelt werden. Auch dieser Entwurf ist vorab inoffiziell veröffentlicht worden.[243] Die Datenschutzbeauftragten des Bundes und der Länder werden zu den offiziellen Entwürfen Stellungnahmen erarbeiten, sobald die Kommission sie beschlossen hat.

Bereits Ende 2010 hat die Kommission ihre Vorstellungen für eine **europäische Strategie der inneren Sicherheit** veröffentlicht.[244] Darin werden neben den schon vorhandenen zahlreichen Datenbanken [EUROPOL, EUROJUST, Schengener Informationssystem (SIS), Zollinformationssystem (CIS), Fingerabdruckdatenbank für Asylbewerber (EURODAC), Visa-Informationssystem (VIS)] die Pläne für zusätzliche eingriffsintensive Datensammlungen erläutert,

241 JB 2010, 11.1
242 Version 56 vom 29. November 2011, in engl. Fassung abrufbar unter www.statewatch.org
243 Version 34 vom 29. November 2011, in engl. Fassung abrufbar unter www.statewatch.org
244 Mitteilung der Kommission an das Europäische Parlament und den Rat vom 22. November 2010, BR-Drs. 772/10

die bis 2014 geplant sind. Diese Pläne enthalten allerdings weder Hinweise auf unabweisbare datenschutzrechtliche Sicherungen noch auf eine dringend notwendige unabhängige Evaluation der schon vorhandenen Datenbanken. Das hatten die deutschen Datenschutzbeauftragten schon 2009 kritisiert.[245] Insofern zeigt sich ein ähnliches Bild wie in der innerdeutschen Diskussion: Statt die Wirksamkeit schon vorhandener Überwachungsstrukturen im Hinblick auf die angestrebten Ziele der Bekämpfung von Terrorismus und schwerer Kriminalität kritisch zu überprüfen, werden ständig neue Strukturen geschaffen, ohne dass bisher wirksame Rechtsschutzgarantien für den Einzelnen auf europäischer Ebene existieren. Auch wird das Prinzip der Datensparsamkeit (Privacy by Default) bei der Konzeption neuer europäischer Datensammlungen weitgehend ignoriert.

So hat der Ministerrat im Dezember einem neuen Abkommen zur **Übermittlung von Fluggastdaten (PNR) in die USA**[246] zugestimmt. Es soll an die Stelle des PNR-Abkommens von 2007 treten und im Gegensatz dazu unbefristet gelten. 19 Daten über jeden Flugpassagier sollen anlassunabhängig an das US-Heimatschutzministerium übermittelt werden, darunter der Name, die Sitzplatz-, Telefon- und Kreditkartennummern der Betroffenen. Die Daten werden in den USA 15 Jahre lang gespeichert und können dort zur Bekämpfung von Terrorismus und Schwerkriminalität genutzt werden. Es bleibt zu hoffen, dass das Europäische Parlament diesem Abkommen die Zustimmung verweigert, denn es ist unvereinbar mit der Europäischen Grundrechte-Charta. Auch das Bundesverfassungsgericht hat 2010 im Zusammenhang mit der Vorratsdatenspeicherung darauf hingewiesen, dass die Freiheitswahrnehmung der Menschen nicht total erfasst und registriert werden darf.

Die **Art. 29-Datenschutzgruppe,** in der wir die Bundesländer vertreten, hat erneut mehrere Papiere verabschiedet. So hat sie sich mit dem überarbeiteten Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen befasst.[247] Die Gruppe hat sich kritisch mit

245 Datenschutzdefizite in Europa auch nach Stockholmer Programm, Dokumentenband 2009, S. 20

246 Vgl. JB 2010, 11.1

247 Stellungnahme 9/2011 vom 11. Februar 2011 (WP 180), im Anschluss an die Stellungnahme 5/2010 vom 13. Juli 2010 (WP 175)

dem Richtlinienvorschlag[248] auseinandergesetzt, der die Verwendung von Fluggastdatensätzen innerhalb der EU vorsieht, und die Erforderlichkeit eines EU-PNR-Systems in Frage gestellt.[249] Angesichts des unterschiedlichen Entwicklungsstandes innerhalb der EU hat sich die Art. 29-Datenschutzgruppe auch zur intelligenten Verbrauchsmessung („Smart Metering") geäußert.[250] Mit einem Arbeitsdokument hat sie darüber hinaus auf der Grundlage der Datenschutzrichtlinie für elektronische Kommunikation die EU-Regeln für Verstöße gegen die Datenschutzvorschriften mit Empfehlungen für künftige Politikentwicklungen (z.B. generelle Informationspflicht bei allgemeinen Datenschutzverstößen) beleuchtet.[251] Schließlich nahm sie Stellung zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten[252] sowie zu den Verhaltensempfehlungen[253], die u. a. von der Europäischen Allianz der Werbeselbstkontrolle[254] zu verhaltensbasierter Werbung im Internet herausgegeben wurden. Ein Grundsatzpapier befasst sich mit den Anforderungen an die Einwilligung.[255]

Erfreulich ist, dass das zunächst schleppend angelaufene **Verfahren zur gegenseitigen Anerkennung von verbindlichen Unternehmensregelungen in der EU (Mutual Recognition)** inzwischen beachtliche Früchte trägt.[256] So sind unter der Federführung der britischen Kollegen die verbindlichen Unternehmensregelungen (Binding Corporate Rules – BCR) der Konzerne Accenture, Atmel, British Petrol, Care Fusion, First Data, General Electric, Hyatt, IMS Health, JP Morgan Chase und Spencer Stuart anerkannt, von der dänischen Aufsichtsbehörde die BCR von Novo Nordisk. Entsprechendes hat die französische Aufsichtsbehörde festgestellt für die verbindlichen Unternehmensregelungen von Bristol-Myers Squibb, Hewlett Packard, Michelin, Safran, Sanofi Aventis und SOS International. Von den holländischen Kollegen wurden die

248 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität vom 2. Februar 2011
249 Stellungnahme 10/2011 vom 5. April 2011 (WP 181), vgl. Dokumentenband 2011, S. 42
250 Stellungnahme 12/2011 vom 4. April 2011 (WP 183), vgl. Dokumentenband 2011, S. 54
251 Arbeitsdokument 1/2011 vom 5. April 2011 (WP 184), vgl. Dokumentenband 2011, S. 74
252 Stellungnahme 13/2011 vom 16. Mai 2011 (WP 185), vgl. Dokumentenband 2011, S. 89
253 Stellungnahme 16/2011 vom 8. Dezember 2011 (WP 188)
254 European Advertising Standards Alliance (EASA)
255 Stellungnahme 15/2011 vom 13. Juli 2011 (WP 187)
256 Zuletzt JB 2009, 11.3

Unternehmensregelungen der Konzerne Sara Lee, Schlumberger und Shell als mit ausreichenden Datenschutzgarantien versehen anerkannt. Die irische Aufsichtsbehörde hat das Anerkennungsverfahren zu den Unternehmensregelungen von Intel abgeschlossen, die luxemburgische Aufsichtsbehörde dasjenige für eBay. Auch Deutschland hat bereits ein europäisches Koordinierungsverfahren federführend betrieben, nämlich für die Unternehmensregelungen der Deutschen Post DHL, für die der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig war.

Bei den Aufsichtsbehörden in Deutschland besteht Einvernehmen, dass trotz des europäischen Mutual Recognition-Verfahrens, bei dem die deutschen Aufsichtsbehörden das Ergebnis der europäischen Federführung „anerkennen", gleichwohl eine innerdeutsche Federführung bestimmt sein muss. Denn diese muss die Informationen aus dem Verfahren (wie das Verfahrensende und die anerkannten BCR) „nach innen zurücktransportieren", d. h. an die übrigen deutschen Aufsichtsbehörden weiterleiten, damit diese entscheiden können, ob und gegenüber wem sie aufsichtsbehördlich (z.B. mit einer Genehmigung nach § 4c Abs. 2 BDSG) tätig werden.

10.2 Genehmigungen für den internationalen Datentransfer

Die Aufzählung zeigt, dass international agierende Konzerne den Datenschutz zunehmend als Marktvorteil begreifen und ihn konzernweit einheitlich regeln wollen. Wir haben auf der Grundlage der von der luxemburgischen Aufsichtsbehörde anerkannten Unternehmensregeln von eBay einer Konzerntochter (brands4friends) zwei Genehmigungen zum Datenexport erteilt und hierfür Gebühren von insgesamt 20.000 € festgesetzt.[257] Entsprechende Bescheide haben wir der KPMG AG sowie einer Tochtergesellschaft erteilt und hierfür Gebühren von insgesamt 24.000 € erhoben. Grundlage dieser Genehmigungen war allerdings nicht eine verbindliche Unternehmensregelung, sondern (wegen der besonderen Unternehmensstruktur) ein sog. Mehrparteienvertrag, den KPMG International und die Mitgliedsfirmen gezeichnet haben.

257 Für Genehmigungen nach § 4c Abs. 2 BDSG ist in Berlin ein Gebührenrahmen von 6.000 – 18.000 € vorgesehen, vgl. Tarifstelle 9104 b) der Anlage zur VGebO (Gebührenverzeichnis)

11. Datenschutzmanagement

11.1 Verhaltensregeln nach § 38a BDSG – Etikettenschwindel vermeiden!

11.1.1 Datenschutz-Kodex für Geodatendienste – keine Abstimmung mit den Aufsichtsbehörden

Unter Federführung des Branchenverbands BITKOM[258], für den wir zuständig sind, entwickelten Anbieter von sog. Panorama-Bilddiensten wie Google („Street View"), Microsoft („Bing Streetside"), Deutsche Telekom, Sidewalk und Panolife einen Entwurf eines Verhaltenskodexes für Geodatendienste. Hierdurch sollten einheitliche Grundsätze für alle Anbieter solcher Dienste in Deutschland etabliert werden. Der Entwurf war bereits Ende 2010 vom BITKOM öffentlich vorgestellt worden[259] und enthielt Regelungen zur Veröffentlichung von Panoramabildern im Internet sowie zur Errichtung einer zentralen Informations- und Widerspruchsstelle. Allerdings blieb der Entwurf in mehreren Punkten hinter den von Google zuvor für den Dienst „Street View" gegebenen Zusicherungen zurück.

Zunächst sah es so aus, als strebe der BITKOM eine Abstimmung mit den Datenschutzaufsichtsbehörden sowie eine rechtliche Verbindlichkeit des Kodexes an. Das BDSG sieht grundsätzlich die Möglichkeit vor, dass Berufsverbände oder andere Vereinigungen Entwürfe für Datenschutzverhaltensregeln der zuständigen Aufsichtsbehörde unterbreiten. Diese kann die Vereinbarkeit mit dem geltenden Datenschutzrecht verbindlich feststellen.[260] Ein Gespräch zwischen den Aufsichtsbehörden und dem BITKOM blieb allerdings erfolglos. Insbesondere griff der BITKOM die zentrale Forderung der Aufsichtsbehörden nach einem Vorabwiderspruch, d. h. der Möglichkeit, einer Veröffentlichung von Häuserfronten im Internet im Vorfeld zu widersprechen, nicht auf.

258 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
259 JB 2010, 1.1.2 (S. 29)
260 Regulierte Selbstregulierung, § 38a BDSG

Stattdessen verzichtete er auf eine Abstimmung mit den Aufsichtsbehörden und überreichte die unterzeichnete Selbstverpflichtung im Rahmen der CeBIT 2011 dem Bundesminister des Innern.

Nach Auffassung der Aufsichtsbehörden entspricht dieser Kodex nicht den datenschutzrechtlichen Anforderungen.[261] Trotz der Beteuerungen des BITKOM, den Dialog mit den Aufsichtsbehörden fortzusetzen, haben keine weiteren Gespräche stattgefunden. Erfreulich ist immerhin, dass sich Microsoft bei „Bing Streetside" letztlich doch entschlossen hat, den Vorabwiderspruch zuzulassen und damit die Anforderungen der Aufsichtsbehörden zu erfüllen, auch wenn dies im Kodex so nicht vorgesehen ist. Dieser hat deshalb weder praktische noch rechtliche Bedeutung.

11.1.2 Datenschutz-Kodex für Internetwerbung

Aus Presseberichten haben wir erfahren, dass der beim Branchenverband ZAW[262] angesiedelte Rat für Datenschutz in der Online-Werbung dabei ist, einen Verhaltenskodex für Internetwerbung zu erarbeiten. Wir haben den ZAW darauf hingewiesen, dass derartige Verhaltensregeln der zuständigen Aufsichtsbehörde zur Prüfung der Vereinbarkeit mit dem geltenden Recht vorzulegen sind[263] und nur nach einem positiven Ergebnis dieser Prüfung rechtliche Bedeutung erlangen können. Wir haben daher dem ZAW ein Orientierungsgespräch angeboten. Der ZAW hat erklärt, dass man ohnehin auf uns zugekommen wäre, jedoch zurzeit noch weitere Abstimmungen erforderlich seien. Es ist zu hoffen, dass die deutsche Werbewirtschaft nicht vergleichbare Fehler begeht wie die entsprechenden europäischen Wirtschaftsverbände.[264]

Bei Verhaltensregeln nach dem Bundesdatenschutzgesetz gilt: Sie müssen einen datenschutzrechtlichen Mehrwert aufweisen. Erst recht darf mit ihnen kein Etikettenschwindel betrieben werden. Wo Datenschutz draufsteht, muss auch Datenschutz drin sein.

261 Beschluss des Düsseldorfer Kreises vom 8. April 2011, Dokumentenband 2011, S. 27
262 Zentralverband der deutschen Werbewirtschaft e.V.
263 § 38a BDSG
264 Siehe 12.1

11.2. Informationspflicht bei Datenpannen

11.2.1 Datenlecks bei öffentlichen Stellen

Seit Februar gilt die mit der Novellierung des BlnDSG eingeführte Informationspflicht bei unrechtmäßiger Kenntniserlangung von Dritten.[265] Diese Pflicht trifft alle Behörden und sonstigen öffentlichen Stellen des Landes Berlin sowie alle landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.[266] Sie müssen sowohl die Datenschutzbehörde als auch die Betroffenen unverzüglich benachrichtigen, wenn personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.[267] Das setzt voraus, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die Betroffenen sind dabei grundsätzlich einzeln zu benachrichtigen. Soweit dies einen unverhältnismäßigen Aufwand erfordern würde, tritt an die Stelle der einzelnen Benachrichtigung eine angemessene Information der Öffentlichkeit. Dies kann z. B. durch Veröffentlichung von mindestens halbseitigen Anzeigen in mehreren Tageszeitungen oder durch andere, gleich wirksame Maßnahmen geschehen. Verstöße gegen die Informationspflicht können beanstandet und die öffentliche Stelle zu einer Stellungnahme aufgefordert werden.[268]

Um die öffentlichen Stellen dabei zu unterstützen, informationspflichtige Vorfälle zu identifizieren und daraus folgende Handlungspflichten umzusetzen, haben wir ein Merkblatt in Form von „Häufig gestellten Fragen“ (FAQs) veröffentlicht.[269]

265 § 18a BlnDSG, vgl. 2.2.1
266 Zur Informationspflicht von nicht-öffentlichen Stellen vgl. § 42a BDSG; JB 2010, 12.2
267 Anders als § 42a BDSG, der nur bestimmte Kategorien von Daten umfasst, schützt § 18a BlnDSG alle personenbezogenen Daten.
268 § 26 Abs. 1 BlnDSG
269 http://www.datenschutz-berlin.de

Wahlbriefe im Hausmüll

Wenige Tage nach der Wahl zum Abgeordnetenhaus war der Presse zu entnehmen, dass ein Anwohner im Hausmüll einer Wohnanlage in Lichterfelde eine Kiste mit 379 ausgefüllten Wahlbriefen gefunden hatte. Einige waren geöffnet worden und deshalb ungültig, die übrigen konnten noch für die Wahl berücksichtigt werden. Das Bezirkswahlamt Steglitz-Zehlendorf teilte uns auf unsere Bitte um Stellungnahme mit, dass vier Wahlbriefe geöffnet worden seien und daher eine Informationspflicht bestehen könne. Weiter teilte man uns mit, die geöffneten Wahlbriefe seien zerrissen gefunden worden, sodass die betroffenen Wählerinnen oder Wähler wohl nicht ermittelt werden könnten. Eine Benachrichtigung könne, wenn überhaupt, erst erfolgen, nachdem die Wahlbriefe von der Polizei zurück an das Bezirkswahlamt übergeben worden seien. Unser Vorschlag, sich von der Polizei die Namen der Betroffenen mit Anschriften übersenden zu lassen, wurde nicht aufgegriffen – deshalb wurden wir ausnahmsweise selbst tätig. Wir erhielten kurzfristig von der Polizei Kopien der sichergestellten Wahlscheine. Wie sich herausstellte, waren sie unversehrt, und es handelte sich nicht um vier, sondern fünf Betroffene. Ihre Benachrichtigung erfolgte erst, nachdem wir unter erneutem Hinweis auf die Informationspflicht die Kopien der Wahlscheine an den Bezirksbürgermeister übersendet hatten.

Das Bezirkswahlamt war verpflichtet, uns sowie die Betroffenen unverzüglich zu benachrichtigen.[270] Bei dem Namen, der Anschrift sowie der abgegebenen Stimme handelt es sich um personenbezogene Daten, die einem Dritten unrechtmäßig zur Kenntnis gelangt sind. Hier hatte jedenfalls der Anwohner, der die Briefe gefunden hatte, Kenntnis von deren Inhalt genommen. Bei besonders sensitiven Daten wie der politischen Einstellung, die sich aus den abgegebenen Stimmen ableiten lässt, ist in der Regel von drohenden schwerwiegenden Beeinträchtigungen auszugehen. Das Bezirkswahlamt ging insoweit auch selbst von einer möglichen Informationspflicht aus. Allerdings hat es nichts zu einer unverzüglichen Benachrichtigung beigetragen. Erst unsere Initiative hat dazu geführt, dass die Betroffenen nach mehr als zwei Monaten seit dem Fund der Wahlbriefe vom Bezirkswahlamt informiert wurden. Dieses

270 § 18a BlnDSG, vgl. 2.2.1

hätte die Kopien der Wahlscheine aber entweder selbst fertigen müssen, bevor der Vorgang an die Strafverfolgungsbehörde abgegeben wurde, oder es hätte Kopien bei dieser anfordern müssen, um der Informationspflicht zu genügen. Jedenfalls konnte die Benachrichtigung der Betroffenen nicht unter Hinweis darauf aufgeschoben werden, dass zunächst der Rücklauf der Unterlagen von der Polizei abgewartet werden müsse. Eine Gefährdung der Strafverfolgung war durch die Benachrichtigung der Betroffenen ohnehin nicht zu befürchten. [271]

Informationspflichtige Stellen müssen alles Zumutbare unternehmen, um der gesetzlichen Pflicht zur unverzüglichen Information des Berliner Beauftragten für Datenschutz und Informationsfreiheit einerseits und der Betroffenen andererseits zu genügen. Wird ein Vorgang an andere Stellen wie Strafverfolgungsbehörden übergeben, muss die informationspflichtige Stelle alles Erforderliche tun, um ihre Informationspflicht zu erfüllen. Dazu müssen Unterlagen ggf. bei der anderen Stelle an- bzw. zurückgefordert werden („Rückholpflicht").

Diebstahl eines Schulsafes

Aus der Praxis

Beim Einbruch in die Erich-Kästner-Grundschule in Steglitz-Zehlendorf wurde u. a. der Schulsafe entwendet, in dem sich ein USB-Stick mit unverschlüsselten Schülerdaten des Vorjahres befand. Dazu gehörten neben dem Namen, der Anschrift und dem Geburtsdatum auch Integrationsmerkmale und Förderschwerpunkte sowie die Angabe, ob die Schülerin oder der Schüler deutscher Herkunftssprache[272] ist. Über die Elternvertretung wurden alle Eltern über den Vorfall sowie die konkret entwendeten Daten informiert, was die Schule bereits in ihrer Meldung an uns angekündigt hatte.

Auf die Frage, ob die Schule dazu verpflichtet war, die Schülerinnen und Schüler bzw. deren Eltern zu informieren, kam es hier nicht mehr an, da die Schule ohnehin benachrichtigt hatte. Es sprach jedoch viel für die Informationspflicht, da in den Schülerdaten besonders sensitive Daten zum Migrationshintergrund und über die Förderschwerpunkte etwa zu Behinderungen enthalten waren.

271 § 18a Abs. 2 BlnDSG

272 Kommunikationssprache innerhalb der Familie ohne Rücksicht auf die Staatsangehörigkeit

Auch musste die Kenntniserlangung durch einen Dritten nicht positiv festgestellt werden, denn es genügt, wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann. Bei gestohlenen USB-Sticks kann davon jedenfalls dann ausgegangen werden, wenn die enthaltenen Daten (wie hier) nicht verschlüsselt sind. Zwar war der USB-Stick im Schulsafe verwahrt, bei lebensnaher Betrachtung kann jedoch davon ausgegangen werden, dass der Safe geöffnet und auf die Daten zugegriffen wurde.

Bei sensitiven Daten ist eine sichere Verschlüsselung auch dann zu empfehlen, wenn der Datenträger in einem Safe aufbewahrt wird.

11.2.2 Datenlecks bei privaten Stellen

Patientenunterlagen im Hausmüll

Ein Journalist übergab uns Patientenunterlagen, die er bei Recherchearbeiten im Hausmüll einer Wohnanlage mit Arztpraxis gefunden hatte (sog. Bin Raiding). Die Unterlagen waren z. T. nur einmal durchgerissen und konnten daher leicht zusammengesetzt werden, z. T. aber auch unversehrt. Es ließen sich nicht nur Namen von Patientinnen und Patienten entnehmen, sondern z. T. auch Diagnosen und verschriebene Medikamente. Wir haben dem Arzt Kopien der Unterlagen überlassen.

Der Arzt war verpflichtet, die betroffenen Patientinnen und Patienten zu informieren, denn es waren personenbezogene Daten, die einem Berufsgeheimnis unterliegen, Dritten unrechtmäßig zur Kenntnis gelangt.[273] Bereits die Tatsache, dass jemand Patient einer bestimmten Arztpraxis ist, ist von der ärztlichen Schweigepflicht umfasst. Neben den Beschäftigen des TV-Senders, die die Unterlagen zur Kenntnis genommen haben, ist bei lebensnaher Betrachtung mit einer gewissen Wahrscheinlichkeit davon auszugehen, dass auch weitere Dritte die Unterlagen im Hausmüll zur Kenntnis genommen haben.

273 § 42a S. 1 Nr. 2 BDSG

Zu der Frage, ob schwerwiegende Beeinträchtigungen für die Rechte und schutzwürdigen Interessen der Betroffenen drohen, hat der Arzt uns mitgeteilt, er könne nicht einschätzen, inwieweit den betroffenen Patientinnen und Patienten durch die Offenbarung ein Schaden entstünde. Hierauf kommt es jedoch bei der Prognose-Entscheidung nicht an. Entscheidend ist allein, ob schwerwiegende Beeinträchtigungen drohen, wovon bei besonders sensitiven Daten wie Patientenunterlagen mit Diagnosen in der Regel auszugehen ist.[274] Wir haben dem Arzt die uns vom TV-Sender überlassenen Unterlagen übersandt, damit er seiner Informationspflicht gegenüber den betroffenen Patientinnen und Patienten nachkommen konnte. Er hat zudem versichert, künftig die sichere Entsorgung von Patientenunterlagen u. a. durch weitere Schredder sicherzustellen.

Patientenunterlagen dürfen keinesfalls ungeschreddert in den Hausmüll gelangen. Ärztinnen und Ärzte haben sicherzustellen, dass alle Beschäftigten entsprechend instruiert werden, und die Einhaltung der Anweisungen regelmäßig zu überprüfen.

Diebstahl der Aktentasche eines Bankmitarbeiters

Aus der Praxis

Ein Bankmitarbeiter stellte auf dem Nachhauseweg seine Aktentasche in einem Schnellimbiss auf einem Stuhl ab, um die Bestellung entgegenzunehmen und zu bezahlen. In diesem Moment wurde die Aktentasche gestohlen, die auch Informationen über Konten und Vermögensverhältnisse von Bankkundinnen und -kunden enthielt. Hierüber hatte die Bank die Betroffenen unverzüglich informiert.

Vorliegend waren personenbezogene Daten zu Bankkonten Dritten unrechtmäßig zur Kenntnis gelangt, sodass unstreitig von einer Informationspflicht auszugehen war.[275] Der Bankmitarbeiter hatte gegen die Richtlinien der Bank verstoßen, nach denen die Beschäftigten vertrauliche Unterlagen außerhalb der Bankgebäude sicher zu verwahren und besonders vor Verlust zu schützen

274 Hier fand sich in den Unterlagen z. B. Name und Anschrift einer Patientin zusammen mit der Diagnose Demenz.

275 § 42a S. 1 Nr. 4 BDSG

haben. Die Bank nahm den Fall zum Anlass, alle Beschäftigten dahingehend zu instruieren, dass nach den Richtlinien Kundenunterlagen mit personenbezogenen Daten nur unter Beachtung besonderer Sorgfaltspflichten außerhalb von Bankgebäuden mitgenommen werden dürfen. Zusätzlich wurde an alle, die über ein dienstliches Notebook verfügen, eine Broschüre über den sicheren Umgang mit Notebooks verteilt.

Beim Transport von vertraulichen Unterlagen ist besonders auf einen sicheren Umgang und eine sichere Verwahrung zu achten. Keinesfalls sollten solche Unterlagen unbeaufsichtigt gelassen werden.

12. Telekommunikation und Medien

12.1 Missachtung von Europarecht bei der gezielten Internetwerbung

Die 2009 geänderte europäische E-Privacy-Richtlinie[276] erfordert die Einwilligung, wenn Anbieter Informationen auf Einrichtungen von Nutzenden zwischenspeichern wollen. Dies betrifft insbesondere die Verwendung sog. **„Cookies“**[277]. Die im April vorgestellte Selbstregulierungsinitiative des Internet Advertising Bureau (IAB) ist mit europäischem Recht nicht vereinbar[278], weil sie im Kern die Widerspruchslösung nach dem vorher geltenden Recht beibehält.[279]

Auch auf nationaler Ebene verzögert sich die Umsetzung in deutsches Recht weiter: Zunächst hatte das Bundeswirtschaftsministerium behauptet, Umsetzungsbedarf ins deutsche Recht bestehe nicht, da die Regelung im nationalen Recht ohnehin schon in der europarechtlich neu festgelegten Form bestehe. Bereits im November 2010 hatten dagegen die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) eine Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste im Telemediengesetz (TMG) gefordert[280].

Wir haben in unserer Stellungnahme zum Gesetzentwurf des Landes Hessen im Bundesrat zur Verbesserung der Privatsphäre bei sozialen Netzwerken angeregt, bei der dort geplanten Änderung des TMG eine entsprechende Regelung aufzunehmen. Der Bundesrat hat diese Anregung aufgegriffen.[281] Es zeichnet

276 Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Dokumentenband 2010, S. 34

277 Vgl. JB 2010, 2.6

278 EASA Best Practice Recommendation on Online Behavioural Advertising, 14. April 2011; http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download

279 Vgl. Stellungnahme der Art. 29-Gruppe 2/2010 (WP 171), Dokumentenband 2010, S. 92; Stellungnahme der Art. 29-Gruppe 16/2011 vom 8. Dezember 2011 (WP 188)

280 Vgl. Dokumentenband 2010, S. 28

281 Vgl. 2.3

sich aber ab, dass die Bundesregierung die Regelung weder in das TMG noch in das Telekommunikationsgesetz (TKG) aufnehmen will. Die Entwicklung ist sicher auch auf die erfolgreiche Lobbyarbeit der Industrie zurückzuführen; dabei gäbe es auch nach der Umsetzung von Artikel 5 Abs. 3 der EU-Richtlinie technische Lösungen, die eine rechtskonforme Verarbeitung personenbezogener Daten für Zwecke der verhaltensbasierten Werbung („targeting marketing“ oder auch „online behavioral advertising“) ermöglichen.

Neuerdings bieten einige Browser die technische Möglichkeit, mit der Nutzende zum Ausdruck bringen können, dass sie eine Verfolgung ihres Nutzungsverhaltens für Werbezwecke nicht wünschen (**„do not track“**). Dieses System geht auf Bemühungen der amerikanischen Verbraucherschutzbehörde (Federal Trade Commission – FTC) zurück, die sich davon einen verbesserten Schutz der Privatsphäre der Nutzenden von Internetdiensten verspricht. Einige der gebräuchlichen Browser erlauben bereits jetzt, eine Einstellung zu wählen, aufgrund derer bei jedem Kontakt zu einer Website in der dorthin gesandten Anfrage eine entsprechende Information übermittelt wird. Auch wenn dieses Verfahren verschiedene Schwächen aufweist, so sind sich die deutschen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich einig, dass das Setzen der entsprechenden Option durch eine Nutzerin oder einen Nutzer der Erklärung eines Widerspruchs im Sinne von § 15 Abs. 3 TMG gleichkommt. Solche Widersprüche sind von Anbietern von Telemedien zu beachten. Technische Verfahren sind so umzugestalten, dass solche Widersprüche erkannt und umgesetzt werden.

Nutzenden kann man bis zur Anpassung des TMG an das geltende Europarecht nur empfehlen, selbst Maßnahmen zum eigenen Schutz zu ergreifen: So erlauben es die meisten am Markt befindlichen Browser, die Verarbeitung von Cookies so zu begrenzen, dass entweder überhaupt keine Cookies akzeptiert werden (was zu Funktionseinbußen in einzelnen Fällen führen kann) oder jedenfalls Cookies von sog. „Drittanbietern“ (dabei handelt es sich vielfach um Online-Werberinge) abgelehnt werden. Alternativ kann auch eine Einstellung gewählt werden, bei der für die Dauer der jeweiligen Sitzung alle Cookies akzeptiert (und die von Drittanbietern abgelehnt), aber nach Ende einer jeden Sitzung gelöscht werden. Letzteres macht zumindest die Verfolgung des Nutzungsverhaltens über verschiedene Sitzungen hinweg und das Wiedererkennen von Nutzenden beim erneuten Besuch einer Seite unmöglich bzw.

erschwert es wesentlich. Allerdings sind neue Verfahren in der Entwicklung, die z. B. aufgrund der jeweils individuellen Einstellungen in den Browsern eine Wiedererkennung anhand eines daraus errechneten Fingerabdrucks (**„Browser Fingerprint“**) ermöglichen. Diese Verfahren sollen gegenwärtig mit ca. 80 % Wahrscheinlichkeit in der Lage sein, einzelne Nutzende zu reidentifizieren. Gegen diese Verfahren ist gegenwärtig kein wirksamer Schutz bekannt. Hier sind die Browserhersteller aufgefordert, entsprechende Gegenmaßnahmen zu ergreifen, damit die Nutzenden die Kontrolle über die weitere Verwendung ihrer Nutzungsdaten zu Werbezwecken zurückerhalten.

Der Bundesgesetzgeber sollte sicherstellen, dass Cookies und andere technische Methoden zur Verfolgung von Nutzenden nur mit deren Einwilligung eingesetzt werden dürfen.

12.2 Datenschutzkonformer Einsatz von Google Analytics

Über zwei Jahre haben die Aufsichtsbehörden des Bundes und der Länder unter Federführung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit mit der US-amerikanischen Google Inc. und der in Hamburg ansässigen Google Germany GmbH Gespräche über die erforderlichen Änderungen zum gesetzeskonformen Einsatz von Google Analytics geführt. Den Hintergrund dafür bildete der Beschluss der Aufsichtsbehörden der Länder zur datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten[282]. Dabei ist es gelungen, folgende wesentliche Verfahrensänderungen zu erreichen:

- Den Nutzenden wird jetzt – wie im Telemediengesetz vorgeschrieben – die Möglichkeit zum Widerspruch gegen die Erfassung von Nutzungsdaten eingeräumt. Google stellt dazu ein sog. Deaktivierungs-Add-On zur Verfügung.[283] Dieses Add-On war bisher für Internet Explorer, Firefox und

282 Dokumentenband 2009, S. 30
283 http://tools.google.com/dlpage/gaoptout?hl=de

Google Chrome verfügbar. Google hat nun Safari und Opera hinzugefügt, sodass alle gängigen Browser berücksichtigt sind. Erhebliche Lücken bestehen aber noch in Bezug auf die in Smartphones verwendeten Browser-Versionen.

- Auf Anforderung des Webseitenbetreibers wird das letzte Oktett der IP-Adresse vor jeglicher Speicherung gelöscht, sodass darüber keine Identifizierung der Nutzerin oder des Nutzers mehr möglich ist. Die Löschung erfolgt in der Regel innerhalb Europas.
- Mit den Webseitenbetreibern soll jetzt ein Vertrag zur Auftragsdatenverarbeitung nach dem BDSG geschlossen werden.

Für Webseitenbetreiber stellt der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit besondere Hinweise zur Verfügung[284]. Ein beanstandungsfreier Betrieb von Google Analytics ist danach möglich, wenn Webseitenbetreiber folgende Punkte umsetzen:

1. Ein Vertrag zur Auftragsdatenverarbeitung[285] muss schriftlich geschlossen werden.
2. Aufklärung der Nutzenden z. B. in der Datenschutzerklärung der Webseite über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics. Zudem muss ein Hinweis auf die Widerspruchsmöglichkeit und ein Link[286] auf das Opt-Out-Add-On eingefügt werden.
3. Einstellungen im Google Analytics-Programmcode müssen verändert werden, um Google mit der Kürzung der IP-Adressen zu beauftragen. Dazu ist auf jeder Internetseite mit Analytics-Einbindung der Trackingcode um die Funktion _anonymizeIp() zu ergänzen.
4. Ein bisher genutzter Analytics-Account muss gelöscht und neu angelegt werden, da Google keine andere Möglichkeit bietet, bisher gespeicherte personenbezogene Daten der Nutzenden zu löschen.

284 http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_Webseitenbetreiber_in_Hamburg.pdf
285 Downloadlink des Vertrages: http://www.google.de/intl/de/analytics/tos.pdf
286 Vgl. Fn. 283

Wir haben öffentlich auf die geänderte Situation hingewiesen und betont, dass neben Google vor allem die Website-Betreiber, die Google Analytics verwenden, für den datenschutzgerechten Einsatz des Produkts verantwortlich sind und unverzüglich die erforderlichen Veränderungen an ihren Angeboten vornehmen müssen. 2012 werden wir die Umsetzung bei in Berlin ansässigen Betreibern von Internet-Angeboten stichprobenartig überprüfen.

Darüber hinaus müssen die technischen Anforderungen des Opt-Out auch auf Smartphones übertragen werden. Hinzu kommt, dass die Entwicklung der Analyse-Software mit dem derzeitigen Stand der Umsetzung keineswegs endgültig abgeschlossen ist. Technische und rechtliche Veränderungen erfordern eine kontinuierliche Weiterentwicklung. So werden die ausstehende Umsetzung der E-Privacy-Richtline, aber auch die Einführung von IPv6 neue Schritte erfordern. Hierzu werden die Aufsichtsbehörden auch weiterhin mit Google im Dialog bleiben.

Auch bei dem Angebot der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e. V. (IVW) zur Reichweitenmessung besteht jetzt eine Widerspruchsmöglichkeit; IP-Adressen der Nutzenden werden zeitnah um das letzte Oktett gekürzt. Auch hier müssen die Anbieter der Websites allerdings entsprechende Verträge mit der IVW zur Auftragsdatenverarbeitung schließen.

Nach langwierigen Verhandlungen kann das Tool zur Web-Reichweitenmessung Google Analytics nun beanstandungsfrei eingesetzt werden. Webseitenbetreiber müssen jedoch einige Punkte beachten bzw. ihre Angebote entsprechend überarbeiten.

12.3 Anonyme Bezahlverfahren

Schon seit mehreren Jahren planen zahlreiche Internetanbieter, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung erhältlich sind. Diese Umstellung des Geschäftsmodells kann mit erheblichen Gefährdungen der Privatsphäre der Nutzenden einhergehen, wenn

personenbeziehbare Daten z. B. über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen. Der Möglichkeit, solche Angebote elektronisch bezahlen zu können bei gleichzeitiger Wahrung von Anonymität oder mindestens Pseudonymität, kommt daher eine gesteigerte Bedeutung zu.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist nicht nur durch das Recht auf informationelle Selbstbestimmung, sondern auch durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Auf einfach-gesetzlicher Ebene ist in § 13 Abs. 6 TMG vorgeschrieben, dass eine Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Die oder der Nutzende ist über diese Möglichkeiten zu informieren.

Allerdings kommen bisher viele Anbieter von Telemedien dieser Verpflichtung nicht oder nur unzureichend nach. Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben daher die Anbieter von Telemedien aufgefordert, ihren gesetzlichen Verpflichtungen nachzukommen.[287] Dabei muss ein Bezahlverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen; es reicht dagegen nicht aus, wenn sich z. B. ein Inhalteanbieter für die Abwicklung der Zahlungsverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Auch die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener „White Cards“ erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können. Das

287 Entschließung vom 22./23. November 2011: Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!, Dokumentenband 2011, S. 33

Kreditwesengesetz[288] regelt zwar in § 25 i KWG neue Sorgfalts- und Organisationspflichten beim Einsatz von elektronischem Geld, dem sog. **E-Geld-Geschäft**[289], enthält aber eine Bagatellgrenze von 100 Euro und verhindert somit die anonyme Bezahlung von kleinen Beträgen nicht.

Im Online-Bereich besteht die grundsätzliche Verpflichtung, eine anonyme oder pseudonyme Zahlungsmöglichkeit anzubieten. Aber guter Datenschutz kann profitabel sein: Die anonyme Bezahlmöglichkeit wird das Online-Geschäft weiter beleben.

12.4 Umgang mit Passwörtern in Webangeboten

Uns erreichten mehrere Hinweise auf Webangebote, deren Nutzerverwaltung nicht dem aktuellen Stand der IT-Sicherheit entsprach. Neben der unverschlüsselten Übertragung von personenbezogenen Daten wurden insbesondere Passwörter im Klartext gespeichert und übertragen. In der Praxis sieht das z. B. so aus: Nach der Anmeldung bei einem Webangebot – z. B. die Einrichtung eines Kundenkontos bei einem Web-Shop – erhält die Kundin oder der Kunde eine Bestätigungsmail des Webangebots, in der alle angegebenen personenbezogenen Daten, ggf. die bestellten Artikel und auch das angegebene Passwort aufgeführt sind. Bei anderen Webangeboten offenbart sich ein laxer Umgang mit personenbezogenen Daten erst bei Nutzung der sog. **Passwort-Vergessen-Funktion,** indem in diesem Fall das ursprüngliche Passwort unverschlüsselt per E-Mail gesendet wird.

Welche Anforderungen sind nun an Webangebote zu stellen? Angesichts der vielfachen Datendiebstähle auch bei großen Internetfirmen, die in diesem Jahr durch die Presse gegangen sind, sollten nach dem Grundsatz der Datensparsamkeit so wenig wie möglich personenbezogene Daten gespeichert werden. Bei Passwörtern ist die Situation noch wesentlich kritischer: Viele Nutzende

288 Geändert durch Artikel 1 des Gesetzes zur Optimierung der Geldwäscheprävention vom 22. Dezember 2011, BGBl. I, S. 2959

289 Man unterscheidet kartengestütztes und softwarebasiertes elektronisches Geld; vgl. dazu die europäische E-Geld-Richtlinie 2000/46/EG

verwenden bei vielen oder allen ihren Accounts dasselbe Passwort – trotz aller gegenteiligen Empfehlungen. Die Betreiber von Webangeboten haben daher so weit wie technisch möglich sicherzustellen, dass diese Passwörter selbst bei einem erfolgreichen Einbruch in die eigene Datenbank nicht gestohlen werden können. Tatsächlich gibt es einige Maßnahmen, die Angreifern den Zugriff auf die Passwörter erheblich erschweren. Die Umsetzung dieser Maßnahmen haben wir bei den oben erwähnten Webangeboten erreicht:

1. Die Passwörter dürfen nicht per E-Mail übertragen werden.
2. Die Passwörter dürfen nicht im Klartext abgespeichert werden, sondern nur als Resultat einer parametrisierten Einwegfunktion über dem Passwort, auch bezeichnet als „salted hash". Durch die kryptographischen Eigenschaften der „Einwegfunktion" ist es praktisch unmöglich, aus den gespeicherten Daten das Passwort (zurück) zu berechnen.
3. Die Passwort-Vergessen-Funktion darf keinesfalls das bisherige Passwort mitteilen, sondern muss dafür sorgen, dass sicher identifizierte Accountinhaber ihr Passwort neu setzen müssen.

Des Weiteren unverzichtbar zum Schutz personenbezogener Daten der Nutzenden sind folgende Maßnahmen, auch wenn sie u. U. höhere Kosten mit sich bringen:

1. Die Umsetzung grundlegender IT-Sicherheitsmaßnahmen, z.B. durch Erstellung und Umsetzung eines IT-Sicherheitskonzeptes, sowie im Fall der Verarbeitung von Daten mit hohem Schutzbedarf die vorherige Durchführung einer Risikoanalyse.
2. Grundsätzliche SSL-Verschlüsselung des Zugangs zumindest zu den personalisierten Teilen des Webangebots. Werden nur Login-Daten verschlüsselt übertragen, besteht die Möglichkeit der zeitweisen Übernahme einer Anmeldung durch einen Angreifer, z.B. indem Session-Cookies etc. abgehört werden.
3. Effektive Methoden zur Prüfung der „Echtheit" eines Nutzers.

Gerade der letzte Punkt ist derzeit im Internet nur schwer zu erreichen. Schon die Nutzung von Nutzername und Passwort – die Nutzenden weisen sich aus,

indem sie nachweisen, ein Geheimnis zu kennen – kann bestenfalls für geringe Sicherheitsanforderungen akzeptiert werden, da vielfach zu einfache Passwörter verwendet werden und diese auch noch unverändert bei vielen verschiedenen Internetangeboten. Auf die Spitze getrieben wird die Unsicherheit, wenn man ein vergessenes Passwort durch die Beantwortung sog. Sicherheitsfragen (z.B. Geburtsname der Mutter) umgehen kann, deren Antwort oft auch für Dritte leicht zu ermitteln ist. Alternativen wären die Verkettung mehrerer Methoden, die Verknüpfung von Besitz und Wissen – wie z.B. den Einsatz der e-ID-Funktion des neuen Personalausweises und die Nutzung unterschiedlicher Kanäle, etwa die Versendung von auf der Webseite anzugebenden Transaktionsnummern per SMS, wie dies beim Online-Banking bereits Standard ist.

Webangebote dürfen personenbezogene Daten niemals unverschlüsselt z. B. per E-Mail versenden, sollten grundsätzlich datensparsam arbeiten und die verbleibenden Daten möglichst verschlüsselt speichern. Passwörter dürfen niemals im Klartext gespeichert werden. Es sind mittelfristig sichere Identifikationstechniken als „Nutzername/Passwort" zu entwickeln, unsichere Passwort-Vergessen-Funktionen sind zu vermeiden.

12.5 Smartphones

Bereits 2010 hatten wir auf Datenschutzprobleme bei Smartphone-Apps hingewiesen[290]. Die Nutzung dieser Geräte hat erneut stark zugenommen. Ebenso hat sich der Nutzungsumfang durch das fast unübersehbare Angebot durch Drittanbieter von Apps für die verschiedenen Systemplattformen ebenfalls erheblich erweitert. Im Hinblick auf die Gewährleistung von Datenschutz und Datensicherheit stehen allerdings viele der am Markt befindlichen Plattformen noch eher am Anfang. Viele App-Stores erheben mehr personenbezogene Daten als eigentlich gesetzlich erlaubt; dies gilt auch und erst recht für die Anbieter von Apps. Darauf hat auch die Stiftung Warentest in einem Testbericht vom August 2011 hingewiesen[291].

290 JB 2010, 2.5

291 Vgl. Stiftung Warentest: Ungeschützter Datenverkehr, Test Nr. 8/2011, S. 42 ff.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben darauf hingewiesen, dass Smartphones im Gegensatz zu herkömmlichen PCs den Nutzenden bisher nur rudimentäre Möglichkeiten bieten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden, häufig werden personenbezogene Daten ohne Wissen der Nutzenden an die Anbieter von Diensten übermittelt.[292] Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein **„Spion in der Hosentasche".** Die Obersten Aufsichtsbehörden fordern daher insbesondere

- eine Verbesserung der Transparenz bezüglich der Preisgabe personenbezogener Daten,
- Steuerungsmöglichkeiten für Nutzerinnen und Nutzer bezüglich der Preisgabe personenbezogener Daten,
- Einflussmöglichkeiten für Nutzerinnen und Nutzer zum Löschen von Spuren bei der Internet-Nutzung über Smartphones, die dort im Gegensatz zu herkömmlichen PCs weitgehend fehlen,
- die Schaffung von Möglichkeiten, Smartphones und die über sie vermittelten Dienste anonym oder unter Pseudonym zu nutzen.

Die Anbieter entsprechender Geräte bzw. Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit muss ernst genommen und umgesetzt werden. Der Schutz der Privatsphäre sollte bereits in die Technologien eingebaut werden (Privacy by Design).

Anbieter von **App-Stores** haben darüber hinaus eine Garantenfunktion im Hinblick auf bestimmte Basiseigenschaften der über den jeweiligen App-Store vertriebenen Anwendung. Dies betrifft vor allem auch Zusicherungen im Hinblick auf die Gewährleistung von Datenschutz und Datensicherheit. Es ist deswegen bedauerlich, dass z.B. Google eine solche Vorabüberprüfung der über die Android-Plattform zur Verfügung gestellten Apps ablehnt. Nutzende sollten

292 Entschließung vom 4./5. Mai 2011: Datenschutzgerechte Smartphone-Nutzung ermöglichen!, Dokumentenband 2011, S. 30

sich darüber informieren, welche Garantien der Anbieter eines App-Stores in Bezug auf Datenschutz und Datensicherheit gibt.

Nicht akzeptabel ist es, wenn Anbieter von Betriebssystemen für Smartphones diese mit versteckten Funktionen anreichern, die hinter dem Rücken der Nutzenden Daten über sie erheben. Im April tauchten Vorwürfe gegen **Apple** auf, nach denen der Hersteller auf den Endgeräten hinter dem Rücken der Nutzenden Bewegungsprofile erstellt habe: Zwei britische Informatiker hatten herausgefunden, dass Mobilfunkgeräte mit dem Betriebssystem iOS 4 Standortdaten der Benutzer über einen Zeitraum von bis zu einem Jahr hinweg unverschlüsselt auf dem Gerät speicherten. Nachdem Apple auf diese Vorwürfe zunächst gar nicht reagiert hatte, sprach das Unternehmen später von einem „Softwarefehler", der mit einem Update behoben wurde. Datenschutzbehörden in Deutschland, aber auch im europäischen und nichteuropäischen Ausland haben dazu Untersuchungen eingeleitet, die z.B. in Südkorea mit der Verhängung einer Geldstrafe endeten. Einige dieser Verfahren sind noch nicht abgeschlossen.

Der Datenschutz bei Smartphones befindet sich noch in den Kinderschuhen. App-Stores und Anbieter von Apps haben insofern eine Bringschuld zu erfüllen.

12.6 Datenschutz in der Unterhaltungselektronik

Die Unterhaltungselektronik ist Technik, die in unseren intimsten Wohnbereichen Verwendung findet. So ist es keine Seltenheit, dass sich Fernsehgeräte und Stereoanlagen im Schlafzimmer befinden, oder ein internetfähiges Radio das Badezimmer verziert. Im Wohnzimmer befindet sich bereits heute ein Sammelsurium an entsprechenden Geräten. Dazu zählen neben den bereits genannten Apparaten ein oder mehrere Spielkonsolen, Tablet-PCs, DVD- und BlueRay-Spieler, der klassische Heim-PC sowie der sog. Media Server, der digitale Fotos, Musik und Videos über das heimische Netzwerk für die diversen Abspielgeräte bereitstellt.

Dabei geht es um Geräte, die Inhalte von externen Anbietern, wie z.B. Fernsehsendern, oder den Inhalt einer DVD zu uns nach Hause transportieren und abspielen. Es entsteht der Eindruck einer kommunikativen Einbahnstraße. Doch entspricht das der Wirklichkeit? Dank breitbandiger Internetzugänge sind die Geräte in der Lage, mit der Außenwelt zu kommunizieren. Damit wird der Zugang zu diversen Mehrwertdiensten des Internets erschlossen. Diese Dienste stellen zusätzliche Informationen über die aktuell verfolgte Sendung zur Verfügung, oder sie bieten Zugriff auf ein breites Spektrum von Videodateien auf diversen Servern verschiedener Anbieter. Diese Dienste sind vielen bereits vom Internetsurfen am Computer vertraut und können nun bequem vom Sofa abgerufen werden.

Der zusätzliche Kanal zum Internet birgt aber auch Gefahren. Diese sind nicht neu, denn sie sind vom heimischen PC bekannt. Neu ist das bedrohte Umfeld, das bisher als sicher angesehen wurde. In der Vergangenheit gab es Vorfälle, die das Gegenteil belegen. Jüngstes Beispiel ist der japanische Elektronikkonzern **Sony**, auf dessen Servern durch Hackerangriffe millionenfach Kundendaten kopiert wurden. Zu den Daten zählten auch Kreditkarteninformationen, die bei einer kriminellen Verwertung für die betroffenen Kunden oder Kreditkartenunternehmen einen wirtschaftlichen Schaden zur Folge hätten. Interessanterweise überwog der Protest bezüglich des Verlusts von „Spiele-Highscores“ und virtuellen Trophäen bei weitem die Empörung über die kompromittierten personenbezogenen Daten. Der Fall zeigt den Vorzug von anonymisierten Bezahlverfahren auf Basis von PrePaid-Karten gegenüber der Hinterlegung von Zahlungsdaten im Internet. Bei Datenpannen lässt sich der persönliche wirtschaftliche Schaden begrenzen.

Die folgenden hypothetischen Szenarien sollen Gefahren veranschaulichen, die von der Nutzung moderner Unterhaltungselektronik ausgehen. Die neueste Generation von Fernsehern, sog. **Smart-TVs**, bieten u. a. die Möglichkeit, Video- oder reine Sprachtelefonate mit der weit verbreiteten Software Skype[293] zu führen. Die Geräte sind dazu zusätzlich mit einer Kamera und einem Mikrofon ausgestattet. Hypothetisch bestünde die Möglichkeit über eine Sicherheitslücke in der Software des Fernsehers sowohl Kamera als auch Mikrofon unbemerkt zu aktivieren und die entstehenden Datenströme auf einem

293 Vgl. JB 2007, 2.3

beliebigen Punkt im Internet zu speichern. So könnte sich etwa das Fitnesstraining der Schwester oder die Aktivität im Elternschlafzimmer auf einer der diversen **Videoplattformen im Internet** – also für jeden abrufbar – wiederfinden. Letztlich könnten auch staatliche Stellen versuchen, diese neuen „Überwachungsmedien" zur Strafverfolgung zu nutzen. Sofern Kamera und Mikrofon als externes Modul bereitgestellt werden, ist ein gewisser Schutz möglich, indem dieses Modul nur im Bedarfsfall mit dem TV verbunden wird. Ansonsten obliegt es der Gerätesoftware, entsprechenden Schutz zu gewährleisten.

Bei Unterhaltungselektronik handelt es sich im Gegensatz zum Heimcomputer in der Regel um ein geschlossenes System. Es ist der Nutzerin oder dem Nutzer nicht möglich, zusätzlichen Schutz zu installieren, da die Software des Fernsehers ausschließlich durch den Hersteller verändert werden kann. Einige Hersteller bieten seit kurzem analog zu den Plattformen für Smartphones die Möglichkeit, zusätzliche Anwendungen (Applikationen, kurz Apps) für das jeweilige Gerät aus dem Internet zu installieren. Diese Vertriebsplattformen werden derzeit nur vom Hersteller des jeweiligen Geräts angeboten. Die bereitgestellten Applikationen unterliegen der Kontrolle der Hersteller. Durch die fehlende Standardisierung der Software für Unterhaltungselektronik sind Applikationen nur in begrenzter Anzahl verfügbar, da ein potentieller Drittanbieter seine Anwendungen auf eine Vielzahl von Geräten anpassen müsste. Verläuft die Entwicklung der Unterhaltungselektronik ähnlich der bei den Mobiltelefonen, so könnte durch eine standardisierte Plattform auch hier eine Überflutung des Markts mit Applikationen diverser Drittanbieter bevorstehen. Es entstünden ähnliche Probleme für den Datenschutz, die aus dem Smartphone-Bereich bekannt sind. [294]

Bereits heute lassen sich einfache Funktionen diverser Geräte wie BlueRay-Player oder Fernseher über eine Applikation auf dem Tablet-PC oder Smartphone steuern. Durch eine in der Zukunft voranschreitende Standardisierung ist es vorstellbar, dass auch Applikationen von Drittanbietern über offene Schnittstellen auf die Geräte zugreifen können. Die Ablösung der Fernbedienung durch den Tablet-PC oder das Smartphone wäre denkbar. Hier ist die Einführung von Sicherheitsmechanismen unerlässlich, die auch technisch unerfahrene Nutzende verstehen und nutzen können. Auch wenn damit eine

294 Vgl. JB 2010, 2.5

gewisse Komplexität einhergeht, sollte der Zugriff von Anwendungen differenziert einstellbar ein. Den Anwender nur vor die Entscheidung zu stellen, ob der Applikation die geforderten Rechte vollständig gewährt werden oder im anderen Fall auf diese komplett zu verzichten, ist unzureichend. Im Ergebnis könnten Programme erscheinen, die neben einer nützlichen Funktion unbemerkt Daten übermitteln oder sogar verändern könnten.

Aktuell erleben wir eine Entwicklung im Bereich der **Vernetzung privater Haushalte,** die mit der Entwicklung in den Betrieben und der Verwaltung in diesem Bereich Anfang der neunziger Jahre vergleichbar ist. Der Unterschied besteht im Wesentlichen darin, dass in der Arbeitswelt erst einzelne Rechner zu lokalen Netzen verbunden wurden. Diese „Netzwerkinseln" wurden sukzessive miteinander vernetzt, sodass die heutigen Netzwerklandschaften entstanden. Private Haushalte beginnen mit einem Internetzugang als Ausgangspunkt für das eigene Wohnungsnetz. Radio- und Fernsehempfang aus dem Netz ist heutzutage kein Problem. Immer mehr Haushaltsgeräte werden folgen. Projekte wie das „Smart Grid" [295] weisen den Weg. An die Sicherheit und den Schutz der Daten wird oft erst in zweiter Linie gedacht. Vorfälle, bei dem Mobiltelefone ab Werk die Standortdaten ihrer Besitzer unbemerkt an den Hersteller übermitteln, sollten daran erinnern, dass die vielen kleinen elektronischen Helfer unseren privaten Bereich ausspionieren können. Es muss nicht immer der große Lauschangriff sein, aber die Summe der einzelnen wissentlich oder unwissentlich übermittelten Daten wächst mit jedem Gerät.

Die Freiheit des Einzelnen, über seine Daten zu bestimmen, muss bereits bei der Entwicklung dieser Technologien gerade auch im Unterhaltungs- und Freizeitbereich beachtet werden. Selbst dann bleibt ein sensibler Umgang der Nutzenden unverzichtbar.

295 Intelligentes Stromnetz, siehe 7.4.1

12.7 IPv6 – das „Internet der Dinge“ kommt

Mit der wachsenden Bedeutung des Internets und der damit einhergehenden zunehmenden Verbreitung von internetfähigen Endgeräten ist gleichzeitig auch der Bedarf an entsprechenden Internet-Adressen gestiegen, damit die einzelnen Geräte innerhalb der jeweiligen Computernetze, die weltweit zum Internet zusammengeschlossen sind, auch adressiert werden können. Technisch wird dies durch das Internet Protokoll (IP) realisiert. Daher werden Internetadressen oft auch als „IP-Adressen“ bezeichnet.

Das bisher verwendete Internet Protokoll Version 4 (IPv4) stellt einen Adressraum von rund vier Milliarden IP-Adressen bereit. In den letzten Jahren hat sich jedoch immer stärker abgezeichnet, dass dieser Adressraum bald erschöpft sein wird, und so hat die Internet Engineering Task Force (IETF) bereits 1998 beschlossen, das Internet Protokoll Version 6 (IPv6) als Nachfolger von IPv4 zu entwickeln, zu testen und schrittweise einzuführen.

Die Einführung von IPv6 bringt neben verschiedenen technischen Vorteilen jedoch sowohl Chancen als auch Risiken in Hinsicht auf den Datenschutz und die Privatsphäre der Nutzenden mit sich. Hierbei sind insbesondere die Konfiguration des neuen Protokolls und die gewählte Strategie für die Zuweisung der jeweiligen IPv6-Adresse zu den einzelnen Nutzenden zu prüfen.

Während aktuell bei IPv4 in den meisten Fällen privaten Endgeräten bei jeder Einwahl ins Internet immer eine neue IP-Adresse zugewiesen wird (dynamische Vergabe von IP-Adressen), bietet IPv6 die Möglichkeit, an jedes mit dem Internet verbundene Gerät dauerhaft eine stets gleichbleibende Internetadresse zu vergeben (statische IP-Adressen-Vergabe). Dies resultiert daraus, dass die Länge der Adressen von ehemals 32 Bit (IPv4) auf 128 Bit steigt (IPv6). Das Internet Protokoll Version 6 verfügt somit über einen Adressraum von rund 340 Sextillionen Adressen – so viele, dass man jedem Sandkorn auf der Erde mehrere IPv6-Adressen zuweisen könnte. Problemlos möglich ist daher, jedem elektronischen Gerät dauerhaft eine weltweit eindeutige Adresse zuzuweisen.[296] Möglich ist damit auch die Adressierung von anderen Gebrauchsgegenständen

296 Detailinformationen finden sich unter http://de.wikipedia.org/wiki/IPv6

z.B. zur Verfolgung von Gepäckstücken, Paketen oder Containern. Man spricht hier – wie bei der RFID-Technologie[297] – vom „Internet der Dinge“.

Dieser technische Vorteil kann sich aus Datenschutzsicht jedoch in einen gravierenden Nachteil verwandeln, da bei einer ggf. über Monate oder sogar Jahre gleichbleibenden IP-Adresse des Geräts einer oder eines einzelnen Nutzenden z.B. die Gefahr besteht, dass Anbieter von Online-Werbung, Medieninhalten oder sozialen Netzwerken Nutzende anhand ihrer IP-Adressen noch einfacher „identifizieren und Aktivitäten […] webseitenübergreifend zu individuellen Profilen zusammenführen können“[298], als dies bisher möglich ist.

Im Gegensatz zu IPv4-Adressen besteht eine IPv6-Adresse aus zwei Teilen. Praktisch wird nur der erste Teil, die ersten 64 Bit, für die Adressierung im Internet verwendet. Der zweite Teil, der sog. Interface Identifier, kann genutzt werden, um Geräte eindeutig zu identifizieren, indem für diesen Adressteil physische Geräteadressen (MAC-Adressen) verwendet werden. Im Heimbereich würden so z.B. der PC, das Smartphone und später ggf. der intelligente Kühlschrank unterschieden. Beide Adressteile ermöglichen die dauerhafte Identifizierung von Gegenständen und Personen, die sie nutzen.

Aufgrund der Spuren, die jeder Einzelne zwangsläufig beim Surfen durch das Internet hinterlässt, und der Fülle an Informationen, die dann einer einzelnen IP-Adresse zugeordnet werden können, besteht hierbei eine große Gefahr des Missbrauchs (z.B. Rückschlüsse auf Vorlieben einer Person und Verwendung der aggregierten Informationen über diese Person für zielgerichtete Werbung ohne Kenntnis und Zustimmung der Betroffenen oder sonstige illegale Nutzung der Daten).

Positiv ist wiederum, dass viele Internetanbieter (Access Provider) das Problem erkannt haben und künftig ihrer Kundschaft in der Regel vermutlich nicht mehr nur eine Adresse, sondern einen ganzen Adressbereich zur Verfügung stellen werden, der dynamisch geändert werden kann. Dadurch wird die Personenbeziehbarkeit des vorderen Teils der IP-Adresse (Präfix) reduziert. Der

297 Vgl. 8.1.6

298 Vgl. hierzu die Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011, Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!, Dokumentenband 2011, S. 23

hintere Teil (Interface Identifier) der Adresse kann für die Geräte im privaten Heimnetz beliebig festgelegt werden. Die Kundin oder der Kunde muss folglich selbst dafür sorgen, dass solche Datenschutzfunktionen aktiviert werden. Ein entsprechendes Verfahren wurde international unter dem Namen IPv6 Privacy Extensions standardisiert, aktuell wird es jedoch noch nicht von allen Endgeräten unterstützt. Daher ist es auch hierbei wichtig, dass sowohl entsprechende Dienste als auch Geräte solche Services unterstützen, am besten von Anfang an nach dem Ansatz „Privacy by Default".

Eines der wesentlichen Ziele bei der Konzeption von IPv6 war es, die Adresskonzepte von IPv4 weiterzuentwickeln, um die Verteilung der Datenpakete (Routing) zu verbessern. Mit IPv6 ist es nun möglich, Daten zielgerichtet zu verteilen, dabei aber die Anzahl der möglichen Routen zu verringern. Dies führt jedoch dazu, dass ähnliche Adress-Präfixe Rückschlüsse „auf ähnliche Routen und damit geografische Herkunft von Datenpaketen" zulassen.[299] Dadurch würde auch die Identifizierung von Nutzenden anhand eines möglicherweise wesentlich genauer bestimmbaren geografischen Orts der genutzten IPv6-Adressen u. U. wesentlich erleichtert werden.

Vor dem Hintergrund der datenschutzrechtlichen Herausforderungen durch die Einführung von IPv6 haben sich sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[300] als auch – nach Vorbereitung durch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group") – die Internationale Konferenz der Datenschutzbeauftragten[301] mit diesem Problem beschäftigt und hierzu detaillierte Empfehlungen erarbeitet. Diese sollen sicherstellen, dass die Chancen, die IPv6 zur Beibehaltung und Verbesserung des gegenwärtigen Datenschutzniveaus bietet, genutzt werden. Derzeit wird innerhalb der „Berlin Group" über einen umfassenden Bericht zu diesen Fragen diskutiert. Hierbei sollen insbesondere die Auswirkungen einer datenschutzfreundlichen Umsetzung von IPv6 auf dem Gebiet der Strafverfolgung untersucht werden.

299 Siehe Entschließung / Dokumentenband wie vor
300 Siehe Entschließung / Dokumentenband wie vor
301 Entschließung vom 1. November 2011 über die Verwendung eindeutiger Kennungen bei der Nutzung der Internet Protokoll Version 6 (IPv6), Dokumentenband 2011, S. 115

Das neue Internetprotokoll IP Version 6 bringt, wenn es richtig eingesetzt wird, auch für die Privatsphäre der Nutzenden Vorteile. Falsch eingesetzt würde es jedoch dazu führen, dass jede oder jeder Nutzende im Internet unter einer dauerhaft gültigen Personenkennzahl identifizierbar wäre. Anonymes Surfen oder Meinungsäußerungen unter einem schützenden Pseudonym wären nicht mehr möglich. Die Beibehaltung der dynamischen IP-Adressvergabe und die Nutzung noch datenschutzfreundlicherer Methoden ist daher von entscheidender Bedeutung. Die zusätzliche Nutzung statischer IP-Adressen für unabhängige Netzangebote ist zu begrüßen und wird dadurch nicht eingeschränkt.

12.8 Aus der Arbeit der „Berlin Group“

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. „Berlin Group“) hat drei Arbeitspapiere verabschiedet:

- Das Arbeitspapier „Datenaufzeichnung in Fahrzeugen“ (Event Data Recording – EDR) behandelt Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller[302].
- Das Arbeitspapier zu Datenschutz und elektronischen Bezahlverfahren für Kleinbeträge („Micropayment“) im Internet weist auf die Notwendigkeit der Bereitstellung anonymer Zahlungsverfahren insbesondere für Medienangebote hin, da diese zunehmend gegen Entgelt angeboten werden und das Fehlen anonymer Zahlungsverfahren die Notwendigkeit einer Identifizierung der oder des Nutzenden allein zum Zwecke der Zahlung nach sich ziehen würde[303].
- Das Arbeitspapier zu „Privacy by Design“ und intelligenten Stromzählern fordert eine Minimierung der Verarbeitung personenbezogener Daten bei der anstehenden Einführung sog. intelligenter Stromnetze („Smart Grids“) zur Wahrung der Privatsphäre der Betroffenen.[304]

302 Dokumentenband 2011, S. 117
303 Dokumentenband 2011, S. 134
304 Dokumentenband 2011, S. 124

Auch die Entschließung der Internationalen Konferenz der Datenschutzbeauftragten über die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6)[305] basiert auf Vorarbeiten von Mitgliedern der Arbeitsgruppe.

Die Arbeitsgruppe hat im September ihre 50. Sitzung in Berlin abgehalten. Sie war 1983 auf Betreiben des ersten Berliner Datenschutzbeauftragten, Dr. Hans-Joachim Kerkau, gegründet worden und hat sich seitdem einen weltweiten Ruf mit ihrer Expertise zum Schutz der Privatsphäre bei Telekommunikation und Medien erworben. Seit 1983 ist eine Vielzahl von gemeinsamen Standpunkten und Arbeitspapieren verabschiedet worden, die teilweise zum jeweiligen Zeitpunkt erstmals bestimmte Eigenschaften von Telekommunikationsnetzen und -diensten sowie Internetangebote unter dem Gesichtspunkt des Datenschutzes analysiert und entsprechende Forderungen an die handelnden Instanzen gestellt haben. Dadurch konnte die Gruppe wertvolle Beiträge zur Verbesserung des Schutzes der Privatsphäre leisten. Diese erfolgreiche Arbeit wollen wir auch in Zukunft fortsetzen.

305 Siehe 12.7, Dokumentenband 2011, S. 115

13. Informationsfreiheit

13.1 Informationsfreiheit in Deutschland

Das **Bundesverwaltungsgericht** hat entschieden, dass das Bundesinformationsfreiheitsgesetz grundsätzlich für die gesamte Tätigkeit der Bundesministerien gilt, denn es unterscheide nicht zwischen dem Verwaltungs- und dem Regierungshandeln eines Ministeriums (hier: der Justiz). Auch komme es nicht darauf an, dass ein Ministerium mit der Abgabe einer Stellungnahme gegenüber dem Petitionsausschuss eine verfassungsrechtliche Pflicht erfülle.[306] Die streitbefangenen Unterlagen betrafen die Reformbedürftigkeit des Kindschaftsrechts sowie solche zur Rehabilitierung der Opfer der sog. Boden- und Industriereform in der damaligen sowjetischen Besatzungszone.[307]

Turnusgemäß tagte die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** unter dem Vorsitz der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen. Vor dem Hintergrund der Planungen zu einem europäischen Register für Produkte, die Nanotechnologie enthalten, forderte die IFK die Bundesregierung auf, sich auf europäischer Ebene für mehr Transparenz gegenüber den Menschen einzusetzen.[308] In einer weiteren Entschließung appellierte die IFK an die Gesetzgeber in Bund und Ländern, flächendeckend allgemeine Regelungen für den Informationszugang zu schaffen und die Ombudsfunktionen der Informationsfreiheitsbeauftragten für Verbraucher-, Umwelt- und sonstige Informationen in Bund und Ländern gesetzlich zu regeln.[309]

Im zweiten Halbjahr fand die Konferenz turnusgemäß beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit statt. In einer Entschlie-

306 Zu einem vergleichbaren Fall in Berlin siehe JB 2006, 11.3.2
307 Urteile vom 3. November 2011 – BVerwG 7 C 3.11 und 4.11
308 Entschließung vom 23. Mai 2011: Geplantes europäisches Nanoproduktregister - Transparenz für Bürgerinnen und Bürger!, vgl. Dokumentenband 2011, S. 137
309 Entschließung vom 23. Mai 2011: Informationsfreiheit – Lücken schließen!, vgl. Dokumentenband 2011, S. 138

ßung trat sie dafür ein, den freien Zugang zu amtlichen Informationen in das Grundgesetz und die Landesverfassungen aufzunehmen; bislang ist dies nur in Brandenburg der Fall.[310]

Der Verbraucherzentrale Bundesverband e. V. hat mit Förderung des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz ein Internetportal eröffnet, in das Verbraucherinnen und Verbraucher ihre Beschwerden über mögliche täuschende **Lebensmittelkennzeichnungen** melden können.[311] Nach Prüfung der Meldung wird der Hersteller um Stellungnahme gebeten und mit der Einschätzung des Portalbetreibers veröffentlicht.

Mit dem Produktsicherheitsgesetz[312] wurde die Rechtsgrundlage für die Veröffentlichung von auch personenbezogenen Informationen[313] im Zusammenhang mit gefährlichen Verbrauchsgütern geschaffen. Ebenfalls geregelt ist der behördliche Informationsaustausch über das europäische **Schnellinformationssystem RAPEX**[314], in dem wöchentlich europaweit über aktuelle Warnungen berichtet wird.

13.2 Informationsfreiheit in Berlin

Die bedeutendste Entwicklung für mehr Transparenz ist zweifelsohne das durch Volksentscheid[315] herbeigeführte **Gesetz**, das den Informationszugang zu den **Privatisierungsverträgen der Berliner Wasserbetriebe** gewährleisten soll;[316] besonders erfreulich ist, dass ausgerechnet zur Informationsfreiheit der erste erfolgreiche Volksentscheid im Land Berlin ergangen ist. Das Gesetz sieht nicht nur die Pflicht zur Bekanntmachung der Verträge, Beschlüsse und

310 Entschließung vom 28. November 2011: Informationsfreiheit ins Grundgesetz und in die Landesverfassungen, vgl. Dokumentenband 2011, S. 139
311 www.lebensmittelklarheit.de
312 Art. 1 des Gesetzes über die Neuordnung des Geräte- und Produktsicherheitsrechts vom 8. November 2011, BGBl. I, S. 2178
313 § 31 ProdSG
314 Rapid Exchange of Information System
315 JB 2010, 14.1 (S. 188 ff.)
316 Gesetz für die vollständige Offenlegung von Geheimverträgen zur Teilprivatisierung der Berliner Wasserbetriebe vom 4. März 2011, GVBl. S. 82

Nebenabreden im Amtsblatt für Berlin vor, sondern auch die Veröffentlichung der Dokumente in unserem Internet-Eingangsportal[317], die umgehend erfolgt ist. Darüber hinaus ist vorgesehen, dass die genannten Dokumente einer „eingehenden, öffentlichen Prüfung und öffentlichen Aussprache durch das Abgeordnetenhaus unter Hinzuziehung von unabhängigen Sachverständigen bedürfen.[318] Hierfür ist im neu gewählten Abgeordnetenhaus der Sonderausschuss „Wasserverträge" eingerichtet worden.

Die Senatsverwaltung für Justiz hat ein neues **Vorschrifteninformationssystem** initiiert, mit dem jeder Mensch die Berliner Gesetze und Rechtsverordnungen im Internet kostenlos abrufen kann.[319] Seit August können Bürgerinnen und Bürger uneingeschränkt auf die Datenbank mit Rundschreiben der Berliner Verwaltung zugreifen.[320] Das soll künftig auch Verwaltungsvorschriften betreffen, die allerdings dezentral von der jeweiligen Verwaltung über das Internet allgemein zugänglich gemacht werden. Damit hat Berlin den Rückstand gegenüber anderen Bundesländern etwas aufgeholt und endlich dafür gesorgt, dass die rechtlichen Grundlagen der Verwaltungsentscheidungen pro-aktiv der Allgemeinheit zur Verfügung gestellt werden.[321] Wünschenswert wäre allerdings, dass Berlin dem Beispiel Bayerns folgen und alle Rundschreiben und Verwaltungsvorschriften zentral veröffentlichen würde. In Bayern treten alle Verwaltungsvorschriften, die nicht innerhalb einer bestimmten Frist veröffentlicht werden, automatisch außer Kraft.

Nach wie vor zu beklagen ist die mangelnde Transparenz beim **Einsatz von Externen** (Lobbyisten) in der Verwaltung[322], zu der der Senat vom Abgeordnetenhaus (bislang erfolglos) aufgefordert wurde.[323] Immerhin wird der Senat künftig in seinen Gesetzesvorlagen an das Abgeordnetenhaus diejenigen Externen namentlich benennen, die auf Anforderung des Senats eine schriftliche Beratungsleistung erbracht haben.[324]

317 § 2
318 § 3 Satz 2
319 www.gesetze.berlin.de
320 www.berlin.de/politik-und-verwaltung/rundschreiben/
321 JB 2008, 15.2.1 (S. 172 f.)
322 JB 2008, 15.1 (S. 168)
323 JB 2010, Anhang 1 Ziff. 5
324 Mitteilung – zur Kenntnisnahme – Von externen Dritten erarbeitete Gesetzesentwürfe kenntlich machen („Footprint"), Abgh.-Drs. 16/4419

Rückschritte hat Berlin allerdings in punkto Lebensmittelüberwachung von Gaststätten gemacht, obwohl der Bezirk Pankow mit dem 2009 als Pilotprojekt gestarteten **Smiley-System**[325] erfolgreich war. Bereits 2010 hatte sich die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz mit den Bezirken darauf verständigt, im Juli 2011 den berlinweiten Smiley einzuführen. Als Vorreiter von Hygienesiegeln im Gaststättenbereich konnte Berlin die Verbraucherschutzministerkonferenz davon überzeugen, dass ein bundeseinheitliches System Anfang 2012 eingeführt wird. Trotz eines von der Senatsverwaltung in Auftrag gegebenen Gutachtens zur Zulässigkeit der Veröffentlichung der Hygieneuntersuchungen im Internet haben einige Bezirke wegen rechtlicher Bedenken wieder von dem Vorhaben Abstand genommen. Möglicherweise hat dazu der zeitgleich zwischen den Verbraucherschutzministern einerseits und den Wirtschaftsministern in Deutschland andererseits naturgemäß auftretende Interessenkonflikt beigetragen, durch den das Vorhaben auf Bundesebene zunächst „ausgebremst" wurde. Dessen ungeachtet hat die Senatsverwaltung im Internet eine Datenbank eingerichtet, in die die Bezirke die Ergebnisse ihrer Lebensmittelkontrollen eingeben können.[326] Als Ergebnisse der Kontrollen werden jeweils der Punktestand und die Note bezogen auf den geprüften Betrieb dargestellt. Damit werden weniger Daten veröffentlicht als im von uns seinerzeit für zulässig befundenen Smiley-System. Pankow beteiligt sich nicht mehr an dieser berlinweiten Website, sondern stellt wie bisher die Ergebnisse seiner Lebensmittelkontrolleure auf der eigenen Bezirksseite ins Internet. Diese Rückkehr zum Alleingang wird maßgeblich damit begründet, dass sich aus der Datenbank nicht ergebe, aus welchem Grund eine Gaststätte gute oder schlechte Noten erhalten hat.

325 JB 2008, 15.2.2
326 www.berlin.de/sicher-essen

13.3 Einzelfälle

Staatsleistungen an Religionsgemeinschaften

Eine Petentin begehrte bei der Senatskanzlei Auskunft zur Höhe der Staatsleistungen an alle Kirchen und sonstigen Religionsgemeinschaften seit Inkrafttreten des Grundgesetzes. Die Senatskanzlei lehnte den Antrag mit der Begründung ab, dass die Zusammenstellung der Leistungen aufgrund der langen Zeitspanne einen unverhältnismäßigen Verwaltungsaufwand bedeuten würde. Darüber hinaus seien die begehrten Informationen im Internet abrufbar.

Wir haben der Senatskanzlei mitgeteilt, dass der Ablehnungsgrund des „unverhältnismäßigen Verwaltungsaufwands“ im Berliner Informationsfreiheitsgesetz (IFG) nicht vorgesehen ist; auch reicht der pauschale Verweis auf die Internet-Veröffentlichung nicht aus, um den Auskunftsanspruch nach dem IFG zu erfüllen. So kann zum einen nicht davon ausgegangen werden, dass jeder Mensch über einen Computer und Internetzugang verfügt. Zum anderen wäre aber der bloße Hinweis, die begehrte Information sei im Internet – irgendwo – abrufbar, ohnehin nicht ausreichend. Jedenfalls wäre die Angabe eines konkreten Links notwendig. Deshalb haben wir um erneute Prüfung des Antrags gebeten und zugleich um Vorabmitteilung, mit welchen Gebühren zu rechnen sei. Diese Prüfung ergab, dass die begehrten Unterlagen nur ab 1994 vorhanden seien und mit einer Gebühr zwischen 220 und 350 € zu rechnen sei. Wir hatten keine Anhaltspunkte dafür, dass dies unverhältnismäßig viel gewesen wäre. Die Petentin nahm daraufhin ihren Antrag zurück, da ihr einerseits die Gebühren zu hoch waren, andererseits die Zusammenstellung ohne den Zeitraum vor 1994 für sie wertlos war.

Eine Behörde kann Akteneinsicht oder Aktenauskunft nicht unter Berufung auf einen unverhältnismäßigen Verwaltungsaufwand ablehnen, denn einen solchen Ablehnungsgrund sieht das Gesetz nicht vor. Der pauschale Verweis auf das Internet ist unzulässig.

Die „Flucht ins Privatrecht“

Zwei Petenten beschwerten sich darüber, dass ihre Anträge auf Akteneinsicht in Bezug auf landeseigene Grundstücke von der Liegenschaftsfonds Berlin GmbH & Co. KG abgelehnt wurden. Zur Begründung wurde darauf verwiesen, dass das Unternehmen nicht dem Anwendungsbereich des IFG unterliege.

Bedauerlicherweise mussten wir den Petenten mitteilen, dass die Ablehnung ihrer Einsichtsbegehren rechtmäßig war. Bei der Liegenschaftsfonds Berlin GmbH & Co. KG handelt es sich um eine juristische Person des Privatrechts und nicht um eine „sonstige öffentliche Stelle“[327], auch wenn sie Aufgaben einer öffentlichen Stelle wahrnimmt. Private unterfallen dem IFG jedoch nur dann, wenn sie mit der Ausübung hoheitlicher Befugnisse betraut sind. Die Liegenschaftsfonds Berlin GmbH & Co. KG betreibt aber reine Grundstücksverwaltung für das Land Berlin und wird insoweit privatrechtlich tätig. Hätte das Land Berlin diese Aufgaben nicht auf eine GmbH ausgelagert, sondern weiterhin von einer öffentlichen Stelle erledigen lassen, wäre der Anwendungsbereich des IFG unzweifelhaft gegeben. Stattdessen führt diese „Flucht ins Privatrecht“ dazu, dass zu der für die Steuerzahlenden interessanten Frage, wie – und vor allem wie kostenträchtig – das Land Berlin seine Grundstücke verwaltet, keine Transparenz hergestellt wird. Das IFG enthält eine Regelungslücke, was wir schon früher kritisiert haben.[328]

Es besteht nach wie vor dringender gesetzgeberischer Handlungsbedarf, damit vermieden wird, dass sich öffentliche Stellen Berlins durch „Flucht ins Privatrecht“ dem IFG entziehen.

327 § 2 Abs. 1 S. 1 IFG
328 JB 2003, 4.9.3 (S. 137)

Notruf bei der Berliner Feuerwehr

Eine Petentin beschwerte sich darüber, dass die Berliner Feuerwehr ihr die Tonaufnahme eines Notrufs nicht herausgeben wollte. Diese Aufnahme benötigte sie für die Prüfung, ob ein Hubschraubereinsatz anlässlich des Todes ihrer Mutter gerechtfertigt gewesen war, da sie für die Kosten dieses Einsatzes aufkommen sollte. Zwar war ihr bereits ein Wortprotokoll des Notrufs übersandt worden, sie hegte jedoch begründete Zweifel, dass es mit der Tonaufnahme übereinstimmte. Die Berliner Feuerwehr begründete die Ablehnung zunächst damit, dass Aufzeichnungen von Notrufen nur zur Strafverfolgung verwendet werden dürfen. Auf den Widerspruch der Petentin wurde die Herausgabe nunmehr mit dem Argument abgelehnt, dass es der Zustimmung der namentlich genannten Anruferin bedürfe, die jedoch telefonisch und postalisch nicht zu ermitteln sei. Kurz nach unserer Intervention hatte jedoch die inzwischen ermittelte Anruferin ihre Zustimmung zur Offenbarung ihres Namens gegeben, sodass der Übersendung der Tonaufnahme nichts mehr entgegenstand.

Da die Anruferin ihre Zustimmung gegeben hatte, kam es in diesem Fall auf eine Interessenabwägung zwischen dem Informationsinteresse einerseits und dem Geheimhaltungsinteresse andererseits nicht an. [329] Die Berliner Feuerwehr hätte ohnehin in jedem Fall prüfen müssen, ob nicht, wie bereits bei dem Wortprotokoll, der Name der Anruferin in der Aufnahme hätte unkenntlich gemacht werden können.[330] Darüber hinaus findet auch die geäußerte Rechtsauffassung, dass Aufzeichnungen von Notrufen nur zur Strafverfolgung verwendet werden dürfen, keine Stütze im Gesetz.

Fraglich blieb, ob die Berliner Feuerwehr für die Übersendung der Tonaufnahme Gebühren hätte erheben dürfen. Akteneinsicht und Aktenauskunft nach dem IFG sind zwar gebührenpflichtig.[331] Die Petentin hatte hier jedoch auch einen datenschutzrechtlichen Auskunftsanspruch, der von der verstorbe-

329 § 6 Abs. 1 IFG
330 § 12 IFG
331 § 16 IFG i. V. m. Tarifstelle 1004 des Gebührenverzeichnisses zur VGebO

nen Mutter durch Rechtsnachfolge auf sie übergegangen war.[332] Ein solcher Anspruch ist im Gegensatz zum Anspruch nach IFG jedoch gebührenfrei.[333] Die Berliner Feuerwehr hat daher von einer Gebührenerhebung abgesehen.

Bei mehreren Anspruchsgrundlagen hat die Behörde die für Antragstellende günstigste Rechtsgrundlage zu wählen. Das gilt auch für die Gebührenfolge.

Gutachten zur Haltung von Zirkustieren

Ein Petent begehrte beim Bezirksamt Charlottenburg-Wilmersdorf Akteneinsicht bezüglich des Gastspiels eines Weihnachtszirkusses im Winter 2009/2010, insbesondere in die Protokolle der Kontrollen, in die Aktenvermerke sowie in das Gutachten eines beauftragten privaten Sachverständigen. Das Bezirksamt teilte dem Petenten mit, nicht mehr über die begehrten Unterlagen zu verfügen. Der Zirkus habe nach dem Gastspiel im Winter 2009/2010 den Zuständigkeitsbereich des Bezirksamts verlassen. Daher habe das Bezirksamt die Akten nebst Gutachten an die nunmehr für die Erteilung der Genehmigung zuständige Behörde übersandt.

Das Bezirksamt war nicht dazu verpflichtet, Akteneinsicht zu gewähren bzw. die Akten wiederzubeschaffen. Der Anspruch auf Informationszugang besteht nur hinsichtlich solcher Akten, die bei der Behörde auch tatsächlich vorhanden sind. Vorliegend waren die Akten jedoch bereits an eine andere Behörde in einem anderen Bundesland abgegeben worden. Eine Pflicht der Behörde zur Wiederbeschaffung von Akten besteht nur dann, wenn diese nach Stellen des Antrags auf Akteneinsicht oder Aktenauskunft abgegeben wurden. Auf Nachfrage versicherte das Bezirksamt, dass die Unterlagen etwa einen Monat vor Antragstellung verschickt worden waren.

332 Zwar ist der datenschutzrechtliche Auskunftsanspruch grundsätzlich höchstpersönlicher Natur und nicht nach § 1922 Abs. 1 BGB vererblich. Ausnahmsweise ist dies jedoch dann möglich, wenn er eine vermögensrechtliche Komponente hat (wie hier die Kosten für den Hubschraubereinsatz).

333 § 16 Abs. 1 BlnDSG

Eine Behörde ist nur dann zur Wiederbeschaffung von abgegebenen Akten verpflichtet, wenn diese zum Zeitpunkt der Stellung des Antrags auf Akteneinsicht oder Aktenauskunft bei der Behörde noch vorhanden waren.

Katalogdaten der öffentlichen Bibliotheken in Mitte

Ein Petent beschwerte sich darüber, dass das Bezirksamt Mitte die beantragte Übersendung von Katalogdaten verschiedener Bibliotheken in Mitte im jeweiligen internen Format abgelehnt hatte. Das Bezirksamt begründete dies zum einen damit, dass die Katalogdaten bereits im Internet veröffentlicht seien, zum anderen mit dem Hinweis auf die Wahrung der berechtigten Schutzinteressen der Lieferanten der Katalogdaten.[334] Da die Katalogdaten käuflich zu erwerben seien, würden den betroffenen Lieferanten durch die Weitergabe ein nicht unwesentlicher wirtschaftlicher Schaden entstehen.

Wir haben dem Petenten mitgeteilt, dass die Rechtsauffassung des Bezirksamts im Ergebnis zutreffend ist und nach dem IFG kein Anspruch auf Herausgabe der Katalogdaten im jeweiligen intern verwendeten Format besteht. Zwar kann bei der Einsicht in Daten, die auf Datenträgern der automatischen Datenverarbeitung gespeichert sind, die Überlassung einer elektronischen Kopie begehrt werden.[335] Im vorliegenden Fall waren die vom Petenten begehrten Daten jedoch tatsächlich bereits im Internet veröffentlich worden, wenn auch nicht in dem vom Petenten gewünschten Format. Nach dem IFG besteht aber kein weitergehender Anspruch darauf, die elektronische Kopie in einem bestimmten Format zu erhalten.

Darüber hinaus stünde der Herausgabe der Katalogdaten aber ohnehin entgegen, dass den Betroffenen durch die Offenbarung ein nicht nur unwesentlicher wirtschaftlicher Schaden entstehen kann.[336] Abweichend von der Auffassung des Bezirksamts waren hier jedoch nicht die jeweiligen Lieferanten der Katalogda-

334 § 7 IFG
335 § 13 Abs. 6 IFG
336 § 7 Satz 1, 2. Alt. IFG

ten die Betroffenen, sondern vielmehr der Verbund der Öffentlichen Bibliotheken von Berlin sowie die Zentral- und Landesbibliothek. Die vom Petenten begehrte Herausgabe der Katalogdaten stand insoweit im Widerspruch zu den Lizenzbestimmungen mit den jeweiligen Lieferanten. Daher wäre allein eine Ausweitung der Lizenz auch auf unbeschränkte Weiterverwendung wie Herausgabe der Rohdaten in Betracht gekommen, die jedoch eine nicht nur unerhebliche Erhöhung der Lizenzgebühren zur Folge gehabt hätte.[337]

Wir konnten dem Petenten jedoch die erfreuliche Mitteilung machen, dass die Deutsche Nationalbibliothek zurzeit dabei ist, ein neues Geschäftsmodell einzuführen. Danach sollen bibliographische Daten künftig kostenlos zur Verfügung gestellt werden, soweit damit keine kostenpflichtigen kommerziellen Produkte erstellt werden.[338]

Das IFG bietet keinen weitergehenden Anspruch darauf, eine elektronische Kopie in einem bestimmten Format zu erhalten, wenn die begehrten Informationen bereits veröffentlicht sind.

Nachhilfe zur Informationsfreiheit beim Bezirksamt Pankow

Aus der Praxis

Ein Petent beantragte beim Bezirksamt Pankow Akteneinsicht in Vorgänge zu zwei Baugenehmigungen. Als der Petent vor Ort Einsicht in eine der Bauakten nehmen wollte, entnahmen Mitarbeiter des Bezirksamts zunächst verschiedene Aktenbestandteile. Auf seine Nachfrage erklärte man ihm, dass es sich dabei um „interne Unterlagen" handle, die ihm nicht offenbart werden müssten. Nach Rücksprache mit uns beantragte er nunmehr Akteneinsicht in die entnommenen Aktenbestandteile. Das Bezirksamt reagierte gegenüber dem Bürger zunächst nicht, erklärte aber uns gegenüber, dass zunächst geprüft werden müsse, ob schutzwürdige Belange Dritter entgegenstünden. Später erhielt der Petent vom Bezirksamt einen Formularvordruck „Antrag auf Gewährung von Akteneinsicht/Auskunft nach dem

337 Ein Verstoß gegen die Lizenzbestimmungen hätte vom Bezirksamt selbstverständlich ebenfalls nicht verlangt werden können.

338 Zu den Einzelheiten siehe www.d-nb.de/service/zd/geschaeftsmodell.htm

Informationsfreiheitsgesetz (IFG)“, in dem ein Feld für die Begründung des Antrags vorgesehen war, mit dem Hinweis, dass eine Akteneinsicht erst nach Zusendung des ausgefüllten Vordrucks erfolgen könne. Zwischenzeitlich hatte der Eigentümer des Grundstücks – eine Stiftung des öffentlichen Rechts des Landes Berlin – zwar seine Zustimmung zur Akteneinsicht erteilt, dies aber nur unter der Bedingung, dass keine Kopien angefertigt werden. Deshalb wurde dem Petenten beim Termin für die Akteneinsicht untersagt, Kopien anzufertigen. Schließlich erhielt der Petent zwei Gebührenbescheide, aus denen sich nicht ergab, wie sich die Gebühr im Einzelnen zusammensetzte.

Angesichts des eskalierenden Streits zwischen allen Beteiligten haben wir die strittigen Unterlagen im Bezirksamt eingesehen und in einem ausführlichen Gespräch die – eindeutige – Rechtslage dargelegt. So konnten wir dem Petenten schließlich zu seinem Recht verhelfen, ohne dass gerichtlicher Rechtschutz erforderlich wurde.

Das Vorgehen des Bezirksamts war in mehrfacher Hinsicht unzulässig. Bei den „internen Unterlagen“ handelte es sich nach Auskunft des Bezirksamtes um reinen Schriftverkehr, etwa mit dem Bauherrn sowie mit anderen Behörden, der keinen sachlichen Aussagewert habe und daher nicht relevant sei. Über die Relevanz von Unterlagen entscheidet aber allein der Petent. Darüber hinaus war der behördliche Entscheidungsprozess abgeschlossen,[339] sodass nichts dagegen sprach, den Schriftverkehr offenzulegen. Es kann für den Bürger durchaus relevant sein zu erfahren, wie eine Entscheidung zustande gekommen ist.

Schutzwürdige Belange Dritter waren nicht zu berücksichtigen, da es sich bei dem Eigentümer des Grundstücks um eine Stiftung des öffentlichen Rechts des Landes Berlin handelte. Diese unterliegt ihrerseits dem IFG, und schützenswerte personenbezogene Daten bzw. Betriebs- oder Geschäftsgeheimnisse enthielten die Unterlagen nicht. Deshalb waren die Einholung der Einwilligung überflüssig und das Kopierverbot unzulässig.

Das gilt auch für die Verwendung des Antragsformulars zur Gewährung von Akteneinsicht, denn dieses implizierte, dass einerseits der Antrag schriftlich

339 § 10 Abs.1 IFG

unter Verwendung des Formulars gestellt und begründet werden, andererseits offengelegt werden muss, in welcher Eigenschaft Antragstellende die Akteneinsicht begehren. Beides ist vom IFG jedoch nicht vorgesehen. So kann der Antrag auf Akteneinsicht sogar mündlich gestellt werden,[340] sodass eine bestimmte Schriftform nicht vorgeschrieben werden darf. Zudem handelt es sich beim Anspruch auf Informationszugang nach dem IFG um einen voraussetzungslosen Anspruch, der nicht begründet werden muss.

Wir haben schließlich erreicht, dass die Gebührenbescheide nachvollziehbar aufgeschlüsselt wurden; die Gebührenhöhe war nicht zu beanstanden.

Auch zwölf Jahre nach Inkrafttreten des Informationsfreiheitsgesetzes gibt es in Berlin noch immer Stellen, die einfachste Fragestellungen nicht richtig beantworten und sich zusätzlich über lange Zeit beratungsresistent zeigen. Der tatsächlich und rechtlich einfache Fall zog sich über fast zehn Monate hin.

Gebühren im Bauaktenarchiv

Aus der Praxis

Das Bezirksamt Pankow fragte bei uns an, ob für die Akteneinsicht im Bauaktenarchiv des Bezirksamts pauschal eine Gebühr von 33 € pro Stunde verlangt werden könne.

Wir haben das Bezirksamt darauf hingewiesen, dass nach den Bestimmungen des Gebührenrechts Verwaltungsgebühren für einzelne Amtshandlungen erhoben werden[341] und unter Berücksichtigung der Kosten des Verwaltungsaufwands, des Werts des Gegenstands der Amtshandlung sowie des Nutzens oder der Bedeutung der Amtshandlung für die Gebührenschuldner zu bemessen sind.[342] Für einfache Akteneinsichten ist dabei eine Rahmengebühr von 5 bis 100 € vorgesehen[343], wobei sich die Gebührenfestsetzung an der im Einzelfall vorgenommenen Amtshandlung bemessen. Es gibt also keine Rechtsgrund-

340 § 13 Abs. 1 IFG
341 § 2 Abs. 1 GebBeitrG
342 § 8 Abs. 2 GebBeitrG
343 Tarifstelle 1004 des Gebührenverzeichnisses zur VGebO

lage dafür, die Gebühr in Form eines pauschalen Betrags festzusetzen. Auch kann die Gebühr nicht als Benutzungsgebühr[344] erhoben werden, da dies so nicht vorgesehen ist.[345] Zusätzlich ist zu bedenken, dass bei der Akteneinsicht in Bauakten häufig zugleich Zugang zu Umweltinformationen gewährt wird, der gebührenfrei ist.[346] Das gilt auch für die Auskunft über die zu einer Person gespeicherten personenbezogenen Daten bzw. Einsicht in Akten mit eigenen personenbezogenen Daten.[347]

Auch für die Einsichtnahme in bezirkliche Bauakten darf eine Gebühr nicht pauschal festgesetzt werden, sondern muss sich am Verwaltungsaufwand orientieren. Das muss insbesondere bei parallellaufenden Akteneinsichten beachtet werden, bei denen sich der Verwaltungsaufwand nahezu auf die Beaufsichtigung der Einsichtnehmenden durch ein und dieselbe Person beschränkt.

Nochmals: BVV-Sitzungen im Internet

Auf Bitte des Bezirksamts Treptow-Köpenick haben wir uns erneut mit der Frage befasst, unter welchen Voraussetzungen öffentliche Sitzungen der Bezirksverordnetenversammlungen (BVV) im Internet übertragen werden dürfen.[348] Insbesondere stand die Frage im Raum, aus welchem Grund gegen den Livestream aus den Sitzungen der BVV Bedenken bestehen, während die Plenarsitzungen des Abgeordnetenhauses übertragen werden.

In einer umfassenden Stellungnahme haben wir nicht nur die Unterschiede zwischen dem Landesparlament und den „Bezirksparlamenten“ herausgearbeitet, sondern auch praktische Hinweise gegeben, deren Beachtung für die rechtmäßige Live-Übertragung von Sitzungen der BVV unerlässlich sind.[349] Diese

344 § 3 GebBeitrG
345 Maßgeblich ist allein Tarifstelle 1004 des Gebührenverzeichnisses zur VGebO.
346 § 18a Abs. 4 S. 3 Nr. 1 IFG
347 § 16 BlnDSG
348 JB 2010, 14.2 (S. 194)
349 Dokumentenband 2011, S. 140

stellen keine Parlamente im staatsrechtlichen Sinne dar, sondern sind als Kollegialorgan der bezirklichen Selbstverwaltung Teil der Exekutive.[350] Damit unterliegen die BVV-Sitzungen – anders als die des Legislativorgans Abgeordnetenhaus – dem Anwendungsbereich des Berliner Datenschutzgesetzes. Mangels Rechtsgrundlage ist die Live-Übertragung von BVV-Sitzungen via Internet nur mit Einwilligung der Betroffenen zulässig.[351] Selbst dann ist die Nutzung solcher kommerziellen Streaming-Dienste problematisch, deren Anbieter die Bilddaten auf Servern in unsicheren Drittstaaten zwischenspeichern oder sich pauschal ein unwiderrufliches Recht zur Weiterverwendung dieser Daten ausbedingen.

Die Bestrebungen nach mehr Transparenz in den Bezirken durch Live-Übertragung der öffentlichen BVV-Sitzungen im Internet sind zu begrüßen; allerdings muss dem Recht auf informationelle Selbstbestimmung der Betroffenen Rechnung getragen werden.

350 Art. 72 Abs. 1 VvB, § 2 BezVG
351 § 6 Abs. 1 Satz 1 BlnDSG

14. Was die Menschen sonst noch von unserer Tätigkeit haben...

Nach den tragischen Ereignissen auf der **Loveparade in Duisburg** am 24. Juli 2010 veröffentlichte die Veranstalterin im Internet neben einem Dokumentarfilm rund drei Stunden ungeschnittene Videoaufzeichnungen von sieben im Zugangsbereich des Veranstaltungsgeländes installierten Überwachungskameras. Teilweise zeigten die Videos Teilnehmerinnen und Teilnehmer, die ausgelassen lachten und scherzten; andere Aufzeichnungen gaben hingegen wieder, wie Menschen in einer Massenpanik zu Tode getrampelt oder teilweise schwer verletzt wurden. Das Geschehen konnte quasi jeden Tag aufs Neue erlebt und umfassend ausgewertet werden. Dies stellte einen intensiven Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung dar. Kein Fernsehsender hätte solche Bilder ausstrahlen dürfen. Wir haben erreicht, dass die Veranstalterin die Videoaufzeichnungen von ihrer Internetseite genommen hat.

Eine Bürgerin sandte dem Vorsitzenden des Landesverbandes ihrer Partei die **Austrittserklärung**. Sie begründete den Austritt mit der wenig zufriedenstellenden Arbeit ihres Ortsverbandes. Sie beschwerte sich bei uns darüber, dass ihr Brief **im Ortsverband unter Nennung ihres Namens** verlesen wurde. Eine Notwendigkeit, die Austrittserklärung der Betroffenen in der Jahreshauptversammlung des Ortsverbandes vorzulesen, bestand nicht. Es hätte genügt, ihre Kritikpunkte ohne Nennung ihres Namens vorzutragen, soweit man im Ortsverband zu dem Ergebnis gekommen wäre, dass die Analyse dieser Kritik für die weitere Arbeit zielführend ist. Wir haben die Partei aufgefordert, künftig in ähnlich gelagerten Fällen auf die Verlesung von Austrittserklärungen zu verzichten, sofern nicht die Auslegung der Austrittserklärung ergibt, dass die Betroffenen dies wünschen.

Ein Bankkunde beschwerte sich darüber, dass Automaten seines Instituts beim Geldabheben automatisch den Kontostand anzeigen. Es bestehe die Gefahr, dass Dritte, die vor dem **Geldautomaten** warten oder den Nachbarautomaten nutzen, seinen **Kontostand** ablesen können. Wir haben der Bank mitgeteilt, dass

die automatische Anzeige des Kontostandes beim Geldabheben nur zulässig ist, wenn durch einen ausreichenden Sichtschutz sichergestellt ist, dass Unbeteiligte die Anzeige nicht einsehen können. Die Bank will dies sicherstellen.

Ein Kreditkarteninhaber beschwerte sich darüber, dass seine Bank ihm mitgeteilt habe, sie habe ihre Kreditkarten-Produktpalette erneuert; er erhalte deshalb eine **Kreditkarte zu neuen Konditionen,** u. a. beinhalte die Karte nun eine **Verkehrsmittelunfallversicherung**. In den AGB befand sich ein Hinweis, mit welcher Versicherung die Bank zusammenarbeitet. Der Bürger fühlte sich von seiner Bank zu Recht schlecht informiert. Wir haben die Bank aufgefordert, künftig bei Eigenschaftserweiterungen von Kreditkarten bei laufenden Verträgen die Betroffenen auf die neuen Datenflüsse (Welche Daten werden zu welchem Zeitpunkt an welche Versicherung übermittelt?) ausdrücklich hinzuweisen.

Ein Bürger bat bei einem **Hörbuch-Download-Portal** um die Löschung seiner zwei eingestellten Buchrezensionen, nachdem ihn ein Personalleiter im **Bewerbungsgespräch** darauf angesprochen hatte. Ein Kundenmitarbeiter des Portals teilte dem Bürger daraufhin mit, dass eine Löschung vom Unternehmen abgelehnt werde, da er unwiderruflich in die Veröffentlichung seines Namens und Vornamens eingewilligt habe. Es stellte sich nach unserer Intervention heraus, dass die erteilten Auskünfte falsch waren und auch nicht der Verfahrensweise des Unternehmens entsprachen. Die beiden Rezensionen hat das Unternehmen unmittelbar nach Erhalt unserer Aufforderung zur Stellungnahme aus seinem Internetangebot entfernt.

Wir wurden darauf aufmerksam gemacht, dass ein Unternehmen auf seiner **Webseite** eine **Liste mit personenbezogenen Daten** ehemaliger Geschäftspartner veröffentlichte, gegen die **offene Forderungen** bestanden. Das Unternehmen begründete dies damit, dass es die Ansprüche zwar gerichtlich geltend gemacht habe, jedoch mangels Zahlungsfähigkeit der Schuldner die entsprechenden Titel nicht vollstrecken konnte und deshalb letztlich sogar die Gerichtskosten selbst zahlen musste. Um andere Unternehmen vor ähnlichen finanziellen Einbußen zu bewahren, habe man sich zur Veröffentlichung einer Schuldnerliste entschlossen. Die Übermittlung personenbezogener Daten von Schuldnern an Dritte kann unter bestimmten Voraussetzungen rechtmäßig sein. Die weltweite Abrufbarkeit solcher Daten im Internet für jedermann ist

jedoch in Anbetracht des schutzwürdigen Interesses der oder des Betroffenen an dem Ausschluss einer solchen Übermittlung in aller Regel, so auch vorliegend, unzulässig. Auf unsere Aufforderung hin hat das Unternehmen die Liste von der Webseite entfernt.

Das **Online-Kontaktformular** einer Berliner Wohnungsgenossenschaft enthielt zahlreiche Datenfelder, die als Pflichtfelder ausgefüllt werden mussten. So wurden Anrede, Name, Straße und Hausnummer, Postleitzahl und Ort sowie die private Telefonnummer abgefragt. Zudem war im Impressum keine E-Mail-Adresse angegeben, sondern es wurde lediglich auf das Kontaktformular verlinkt. Daher war keine Kontaktaufnahme über das Internet ohne die Angabe der geforderten Daten möglich. Für eine Kontaktaufnahme über das Internet sind vor allem bei Erstinteressenten insbesondere die **vollständige Anschrift und private Telefonnummer** nicht notwendig. Das Wohnungsunternehmen hat unsere Hinweise zum Anlass genommen, das Kontaktformular zu überarbeiten. Nunmehr müssen nur noch Anrede und Name angegeben werden. Wenn die weiteren Felder nicht ausgefüllt werden, wird auf die Freiwilligkeit der fehlenden Angaben hingewiesen. Die Kontaktanfrage kann aber nun auch ohne diese Angaben verschickt werden. Da daneben die Möglichkeit zur Kontaktaufnahme per Telefon oder Fax besteht, erfolgt die Angabe des Namens und der Anrede im Kontaktformular freiwillig.

Ein Bürger beschwerte sich darüber, dass eine Auskunftei zur Einholung einer **Eigenauskunft**[352] auch **bei persönlicher Vorsprache** des Antragstellers zum Identitätsnachweis eine **Ablichtung des Personalausweise**s anfertigt und aufbewahrt. Die Auskunftei begründete diese Praxis damit, dass die Ausweiskopie als Nachweis bei späteren Streitigkeiten über die Berechtigung zur Auskunftserteilung notwendig sei. Zwar ist die Vorlage eines Identitätsnachweises zur Prüfung einer Anspruchsberechtigung in der Regel erforderlich. Jedoch kann bei persönlichem Erscheinen des Antragstellers die Identität eindeutig festgestellt werden. Die Anfertigung und Aufbewahrung einer Kopie des Personalausweises ist in diesem Fall nicht erforderlich und somit unzulässig. Wir haben der Auskunftei empfohlen, als zusätzliche Sicherungsmaßnahme die Identität von Antragstellenden im Wege des Vier-Augen-Prinzips zu prüfen. Die Aus-

352 Vgl. § 34 BDSG

kunftei ist unserer Empfehlung gefolgt und wird künftig keine Ausweiskopien bei der persönlichen Einholung einer Eigenauskunft erstellen.

Ein Empfänger von Leistungen nach dem Sozialgesetzbuch Zwölftes Buch (SGB XII) musste sich zwecks Überprüfung seiner Umzugsfähigkeit einer **ärztlichen Untersuchung** unterziehen. In diesem Zusammenhang wurde der begutachtenden Ärztin vom zuständigen Leistungsträger, dem Bezirksamt Charlottenburg-Wilmersdorf, die **Höhe des aktuellen Mietzinses** der von dem Leistungsempfänger bewohnten Wohnung mitgeteilt. Diese Datenübermittlung war unzulässig. Um klären zu können, ob ein Leistungsempfänger körperlich zu einem Umzug in der Lage ist, spielen ausschließlich Gesundheitsdaten eine Rolle. Die Höhe des Mietzinses ist für die Beurteilung der Frage, ob dem Leistungsempfänger aufgrund seines Gesundheitszustandes ein Umzug in eine andere Wohnung zugemutet werden kann, nicht erforderlich. Das Bezirksamt wird unserer Empfehlung folgen und künftig bei entsprechenden Untersuchungsaufträgen von der Übermittlung der Mietzinshöhe absehen.

Wir konnten erreichen, dass die Senatsverwaltung für Integration, Arbeit und Soziales das Formular für die **Beantragung eines finanziellen Mehrbedarfs für krankheitsbedingte kostenaufwändige Ernährung** überarbeitet und um einen Hinweis auf das Bestehen eines **Alternativverfahrens** ergänzt. Mit dem überarbeiteten Formular haben die Leistungsempfangenden wie bisher die Möglichkeit, eine Schweigepflichtentbindungs- und Einwilligungserklärung abzugeben, wenn sie sich nicht selbst um das Einreichen der erforderlichen medizinischen Unterlagen kümmern wollen. In diesen Fällen kann der jeweilige Leistungsträger direkt an die behandelnde Ärztin bzw. den behandelnden Arzt herantreten und die benötigten Informationen erheben. Für diejenigen Leistungsempfangenden, die mit einer derartigen Verfahrensweise nicht einverstanden sind, enthält die überarbeitete Fassung des Formulars jetzt einen Hinweis darauf, dass sie alternativ die Möglichkeit haben, die benötigten Informationen selbst bei ihrer behandelnden Ärztin bzw. ihrem behandelnden Arzt einzuholen und an den zuständigen Leistungsträger weiterzugeben.

Eine Bürgerin machte uns darauf aufmerksam, dass die **Ärztekammer Berlin** auf ihrer Homepage dazu auffordert, **Beschwerden per E-Mail** als einen möglichen Weg der Kontaktaufnahme an die Ärztekammer zu senden. Dadurch bestand die Gefahr, dass ggf. auch sensible Gesundheitsdaten per E-Mail ver-

sendet würden. Wir konnten die Ärztekammer davon überzeugen, einen Hinweis auf die Homepage zu setzen, mit dem die Betroffenen darauf aufmerksam gemacht werden, dass eine Vertraulichkeit der Daten mit der Versendung per E-Mail nicht gewährleistet ist. Darüber hinaus hat die Ärztekammer die Datenschutzerklärung so geändert, dass darauf hingewiesen wird, dass Beschwerdeschreiben mit schützenswerten Gesundheitsdaten nicht per E-Mail übermittelt werden sollen, da die Vertraulichkeit und die Identität der Beteiligten nicht gewährleistet werden kann.

Ein Ehepaar erhielt vom Finanzamt Steglitz unter Bezugnahme auf einen **Runderlass der Senatsverwaltung für Finanzen** die Aufforderung, einen Ausstattungsbogen sowie eine Baubeschreibung zu übersenden. Der Antrag des Ehepaars auf Einsichtnahme in den Runderlass wurde vom Finanzamt mit der Begründung abgelehnt, das IFG betreffe nur allgemeine Verwaltungsangelegenheiten, und die Finanzgerichtsbarkeit sei davon ausgenommen. Auf unseren Vorhalt, dass das Finanzamt nicht zur Finanzgerichtsbarkeit gehöre, wurde erklärt, dass das IFG auch auf Finanzämter nicht anwendbar sei. Zudem trage der Runderlass den Vermerk „nicht zu veröffentlichen". Nach ausführlicher Erläuterung der eindeutigen Rechtslage konnten wir das Finanzamt zur Herausgabe des begehrten Dokuments bewegen.

Ein Bürger begehrte von der **Senatsverwaltung für Wirtschaft, Technologie und Frauen** die **Übersendung einer Studie,** die in das „Energiekonzept 2020" eingeflossen war. Dem Bürger wurde zunächst mitgeteilt, dass die Studie im Rahmen des Energiekonzepts veröffentlicht würde, allerdings könne man ihm nicht sagen, wann mit einer Fertigstellung des Konzepts zu rechnen sei. Die Senatsverwaltung teilte uns auf Nachfrage mit, dass sie das Energiekonzept zwischenzeitlich auf ihrer Webseite veröffentlicht habe und die begehrte Studie dort ebenfalls enthalten sei. Eine Überprüfung durch uns ergab jedoch, dass ausgerechnet die vom Bürger begehrte Studie zwar im Anlagenverzeichnis zum Energiekonzept aufgeführt, jedoch weder auf der Webseite noch in der Druckfassung veröffentlicht war. Eine erneute Nachfrage bei der Senatsverwaltung führte dazu, dass die Studie kurz darauf auf der Webseite veröffentlicht wurde.

Ein Bürger begehrte bei den **Berliner Forsten** Einsicht in Unterlagen zu einer Waldumwandlungsgenehmigung zugunsten einer Stiftung des öffentlichen Rechts des Landes Berlin. Die Berliner Forsten forderten den Bürger

zunächst auf, den Antrag auf Akteneinsicht zu begründen, und wiesen darauf hin, dass die Akteneinsicht kostenpflichtig sei. Daraufhin vereinbarte der Bürger zunächst einen Termin für die Akteneinsicht, der jedoch von den Berliner Forsten wieder abgesagt wurde. In der Folge wurde dem Bürger mitgeteilt, dass Betriebs-/Geschäftsgeheimnisse[353] der Stiftung entgegenstünden, da wichtige Bauunterlagen Teil des Verwaltungsvorgangs seien. Wir teilten den Berliner Forsten mit, dass für Umweltinformationen nicht das IFG, sondern das UIG anwendbar ist[354] und Akteneinsichten in Umweltinformationen vor Ort gebührenfrei sind.[355] Auf den Einwand der Berliner Forsten, dass der Bürger sich selbst auf das IFG berufen habe, erklärten wir, dass die öffentliche Stelle selber prüfen muss, welche Anspruchsgrundlage die richtige ist.[356] Zudem wiesen wir darauf hin, dass die durch die Waldumwandlungsgenehmigung Begünstigte eine Stiftung des öffentlichen Rechts des Landes Berlin ist, die ihrerseits dem IFG unterliegt und sich nicht ohne Weiteres auf eigene schützenswerte Betriebs-/Geschäftsgeheimnisse berufen kann. Nach unserer Intervention wurde die begehrte Akteneinsicht in vollem Umfang gewährt.

Eine Bürgerin begehrte beim Ordnungsamt des Bezirksamts Charlottenburg-Wilmersdorf die **Übersendung von Kopien** über die **Prüfung einer Gaststätte wegen Geruchsbelästigung.** Sie habe vom Bezirksamt widersprüchliche Aussagen darüber erhalten, ob ihr ein solches Recht zustehe und ob Gebühren erhoben werden. Unsere Nachfrage beim Bezirksamt ergab, dass der Bürgerin Akteneinsicht in den Räumlichkeiten des Bezirksamts gewährt werden würde. Gegen die Übersendung von Kopien bestünden Bedenken, da dann die Verwaltung die offenzulegenden Aktenbestandteile auswähle und die Bürgerin entgegenhalten könne, dass die Auskunft nicht vollständig sei. Wir erklärten, dass die Bürgerin ihr Anliegen so klar eingegrenzt habe, dass einer Übersendung von Kopien nichts entgegensteht. Sollte die Bürgerin gleichwohl Zweifel an der Vollständigkeit haben, so stehe es ihr frei, vor Ort Akteneinsicht zu nehmen. Das Bezirksamt übersandte der Bürgerin daraufhin die begehrten Aktenauszüge, wofür geringe Kopier- und Zustellungsgebühren erhoben wurden.

353 § 7 IFG
354 § 18a Abs. 1 IFG
355 § 18a Abs. 4 Satz 3 Nr. 1 IFG
356 JB 2010, 14.2 (S. 191 f.)

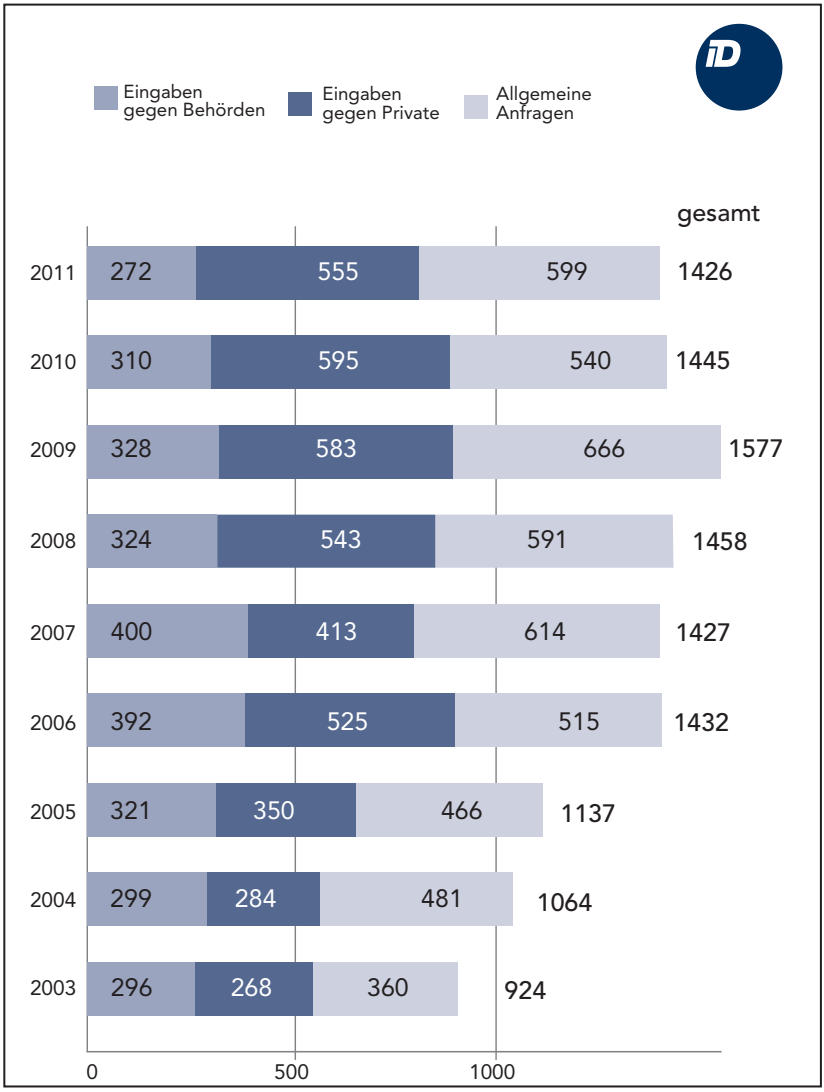
15. Aus der Dienststelle

15.1 Entwicklungen

Die zunehmende Bedeutung des Datenschutzes schlägt sich auch in einem Aufgabenzuwachs für unsere Dienststelle nieder. Die Koordinationsarbeit, die wir seit jeher auf nationaler und internationaler Ebene im Bereich der Telekommunikation leisten, wird in dem Maße wichtiger, wie Internetunternehmen (z. B. Google und Facebook) durch ihre Aktivitäten in Deutschland und Berlin datenschutzrechtliche Fragen aufwerfen. Wir haben in diesem Zusammenhang als Vorsitzland in der Arbeitsgruppe Telekommunikation und Telemedien des Düsseldorfer Kreises den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit in seinen Bemühungen unterstützt, datenschutzrechtliche Verbesserungen im Angebot der beiden genannten US-Unternehmen zu erreichen, was jedenfalls bei Google Analytics gelungen ist.[357] Zugleich sind wir bestrebt, gerade auch die jungen Unternehmen zu beraten, die in Berlin im Bereich der Internetdienstleistungen und Mobilkommunikation zu einem „Start-up-Boom“ beigetragen haben.

Die Zahl der Eingaben, mit denen Bürgerinnen und Bürger sich an uns wenden, liegt nach wie vor auf einem gleichbleibend hohen Niveau. Interessant ist dabei, dass die Zahl der Eingaben gegen Unternehmen mehr als doppelt so hoch ist wie die Zahl der Beschwerden gegen Behörden.[358] Wir haben im Berichtszeitraum wegen Verstößen gegen das Bundesdatenschutzgesetz Bußgelder in Höhe von insgesamt 22.705 Euro festgesetzt und Bußgelder in Höhe von 14.951,82 Euro eingenommen.

357 Vgl. 12.2
358 Vgl. Grafik nächste Seite



Anzahl der Bürgereingaben im Jahresvergleich

15.2 Zusammenarbeit mit dem Abgeordnetenhaus

Im Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses sind der Jahresbericht 2009 und die Stellungnahme des Senats[359] beraten und mit Beschlussempfehlungen versehen worden. Diese Empfehlungen hat das Abgeordnetenhaus am 23. Juni 2011 angenommen.[360] Das Verfahren hat sich in den zurückliegenden Jahren bewährt. Berlin folgt damit dem Beispiel des Deutschen Bundestages, der die Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Beratungen im Innenausschuss zum Anlass für Beschlüsse nimmt, in denen die Verwaltung, aber auch die Wirtschaft zu Verbesserungen gerade im Bereich des Datenschutzes aufgefordert wird. Außerdem wurden im Unterausschuss „Datenschutz und Informationsfreiheit“ mehrere Gesetzgebungsvorhaben (z. B. die Novellierung des Berliner Datenschutzgesetzes und des Landeskrankenhausgesetzes sowie das Strafvollzugsdatenschutzgesetz)[361] sowie zahlreiche aktuelle Fragen des Datenschutzes und der Informationsfreiheit behandelt.

15.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** tagte am 16./17. März in Würzburg und am 28./29. September in München unter dem Vorsitz des Bayerischen Landesbeauftragten für den Datenschutz. Dabei wurden zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes gefasst.[362] Für 2012 hat die Brandenburgische Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht den Vorsitz in der Konferenz übernommen.

Die im **Düsseldorfer Kreis** kooperierenden Aufsichtsbehörden für den **Datenschutz im nicht-öffentlichen Bereich** haben unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

359 Abgh.-Drs. 16/4334
360 Vgl. Anhang 1
361 Vgl. 2.2
362 Vgl. Dokumentenband 2011, S. 9 ff.

am 4./5. Mai und am 22./23. November in Düsseldorf getagt und jeweils Entschließungen zu aktuellen Fragen des Datenschutzes im Unternehmensbereich gefasst.[363] Auch 2012 wird der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen weiterhin den Vorsitz im Düsseldorfer Kreis führen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, deren Mitglieder mittlerweile fast alle[364] zugleich Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sind, hat sich allerdings darauf verständigt, den Düsseldorfer Kreis und seine Arbeitsgruppen in die Konferenz zu integrieren, um auf diese Weise die Kräfte stärker zu bündeln.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 23. Mai unter dem Vorsitz der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen in Bremen und am 28. November in Berlin unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Auch diese Konferenz hat Entschließungen zu aktuellen Fragen des Informationszugangs und der Transparenz gefasst.[365] Im ersten Halbjahr 2012 hat der Landesbeauftragte für den Datenschutz Rheinland-Pfalz den Vorsitz in dieser Konferenz inne.

Seit jeher vertritt Berlin die Bundesländer im Auftrag der Konferenz der Datenschutzbeauftragten und der Aufsichtsbehörden in der **Arbeitsgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie.** Diese Gruppe, die im Zuge der Neugestaltung des Europäischen Rechtsrahmens an Bedeutung gewinnen wird, hat erneut mehrere wichtige Arbeitspapiere und Stellungnahmen verfasst, von denen ein Teil in unserem Dokumentenband veröffentlicht ist.[366] Auf Einladung des Vorsitzenden der Art. 29-Gruppe und des Europäischen Datenschutzbeauftragten fand die **Europäische Konferenz der Datenschutzbeauftragten** am 5. April in Brüssel statt. Unter dem Vorsitz der Mexikanischen Kommission für den Informationszugang fand die **33. Internationale Konferenz der Datenschutzbeauftragten** vom 2. bis 4. November in Mexiko-Stadt statt. Sie fasste u. a. eine Entschließung zu den Datenschutzproblemen im Zusammenhang mit dem neuen Internetprotokoll IPv6, die

363 Vgl. Dokumentenband 2011, S. 28 ff.
364 Mit Ausnahme des Bayerischen Landesbeauftragten für den Datenschutz
365 Vgl. Dokumentenband 2011, S. 137 ff.
366 Vgl. Dokumentenband 2011, S. 42 ff.

wesentlich von der **Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation („BerlinGroup“)** vorbereitet worden war.

Diese Arbeitsgruppe tagte unter unserem Vorsitz am 4./5. April in Montreal; am 12./13. September trat sie zu ihrer 50. Sitzung in Berlin zusammen.[367] Die Gruppe verabschiedete mehrere Arbeitspapiere, die ihrerseits Einfluss z. B. auf die Arbeiten der Art. 29-Gruppe hatten.[368]

Außerdem besuchten im Berichtszeitraum mehrere ausländische Delegationen die Dienststelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Erfahrungsaustausch. Neben einer Delegation aus der Volksrepublik China kamen Vertreter der Datenschutzbehörden aus Mazedonien, Moldawien und Norwegen. Mit den in Mazedonien für den Datenschutz und die Informationsfreiheit zuständigen Behörden wurde eine engere Zusammenarbeit vereinbart.

15.4 Öffentlichkeitsarbeit

Am 28. Januar fand zum Thema „Datenschutz in Europa – Quo vadis?“ in der Vertretung des Landes Baden-Württemberg beim Bund in Berlin der 5. Europäische Datenschutztag statt.

Am 19. Mai führten wir mit dem Institut für das Recht der Informations- und Kommunikationstechnik der Juristischen Fakultät der Humboldt-Universität zu Berlin eine Veranstaltung durch zum Thema „Entweder wir beachten den Datenschutz oder Alle wissen von Allen Alles“. Im Vordergrund stand die Gesamtsituation der informationellen Selbstbestimmung.

Am 24. Juni haben wir für zahlreiche Vertreterinnen und Vertreter aus dem Krankenhausbereich eine Tagung initiiert, die der Erläuterung der von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossenen „Orientierungshilfe Krankenhausinformationssysteme“ diente.

367 Vgl. dazu 12.8
368 Vgl. Dokumentenband 2011, S. 117 ff.

Mit der Europäischen Akademie für Informationsfreiheit und Datenschutz führten wir am 27. Juni eine Diskussionsveranstaltung der sog. Zukunftswerkstatt zu „Transparenz und Privacy“ und am 17. Oktober zum neuen europäischen Rechtsrahmen durch.

Außerdem beteiligten wir uns an folgenden öffentlichen Veranstaltungen:

- „Cybermobbing“/Informationstage für pädagogische Fachkräfte am 16. und 30. Mai
- Tag der offenen Tür im Abgeordnetenhaus am 28. Mai
- 7. Jugendverbraucherschutztag unter dem Motto „Gut informiert & bewusst entscheiden“ im Freizeit- und Erholungszentrum Wuhlheide am 15. September
- Jugendmesse YOU unter dem Motto „Wie vernetzt bist du?“ am 23./24. September in den Messehallen am Funkturm.

Berlin, den 28. März 2012

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Anhänge

Anhang 1:
Beschlüsse des Abgeordnetenhauses vom 23. Juni 2011

Anhang 2:
Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 23. Juni 2011 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2009

Stichwortverzeichnis

Beschlüsse des Abgeordnetenhauses vom 23. Juni 2011

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2009

1. Auch Kranke brauchen Datenschutz – Zugriffsregelungen in Krankenhausinformationssystemen (2.3, Drs S. 32 ff)

Der Senat wird aufgefordert, darauf hinzuwirken, dass beim Einsatz von Krankenhausinformationssystemen in den Berliner Krankenhäusern das Patientengeheimnis sichergestellt wird. Der Zugriff auf die personenbezogenen Daten von Patientinnen und Patienten darf technisch und organisatorisch nur ermöglicht werden, wenn und soweit dies für ihre optimale Behandlung oder für die korrekte Abrechnung der an ihnen erbrachten Leistungen erforderlich ist. Kontrollen haben auch in Berlin ergeben, dass die Zugriffsmöglichkeiten des Krankenhauspersonals auf die elektronischen Krankenakten in den meisten Krankenhäusern weit über das notwendige Maß hinausgehen. Für die Behebung dieser Mängel steht seit Neuem eine Orientierungshilfe zur datenschutzgerechten Gestaltung von Krankenhausinformationssystemen zur Verfügung, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und von den obersten Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft vorgelegt wurde.

2. Kfz-Kennzeichenscanning (3.1, Drs S. 46 ff)

Der Senat wird aufgefordert, bis zur Schaffung einer speziellen Rechtsgrundlage sicherzustellen, dass beim Einsatz eines Kfz-Kennzeichenlesegerätes auf der Grundlage von § 25 Abs. 1 S. 1 Nr. 2 ASOG Aufzeichnungen betreffend Personen, gegen die sich die Datenerhebungen nicht richteten, unverzüglich und soweit technisch möglich automatisch gelöscht werden, soweit sie nicht zur Strafverfolgung benötigt werden.

3. Leichtathletik-Weltmeisterschaft (3.3, Drs S. 49 ff)

Der Senat wird aufgefordert, bei der nächsten Senatsvorlage zu einer Änderung des ASOG eine klarstellende Regelung für Zuverlässigkeitsprüfungen und Akkreditierungsverfahren bei Großereignissen vorzusehen und bis dahin den Umfang von Zuverlässigkeitsprüfungen auf das unabdingbar notwendige Maß zu beschränken, was insbesondere eine Differenzierung der zu überprüfenden Personen nach ihrer Funktion und ihrer Zutrittsrechte zu sicherheitssensiblen Bereichen beinhalten kann. Bei der Erstellung von Konzepten zur Zuverlässigkeitsprüfung ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit einzubeziehen.

4. Videoüberwachung von Demonstrationen (3.5, Drs S. 53 ff)

Der Senat wird aufgefordert, den Unterausschuss für Datenschutz und Informationsfreiheit über den Ausgang des Verfahrens vor dem OVG Berlin-Brandenburg betreffend die Nichtzulassungsbeschwerde gegen das Urteil des VG Berlin vom 5. Juli 2010 (VG 1 K 905.09) zu informieren und bis zu dieser Entscheidung auf polizeiliche Videobeobachtung von Demonstrationen zur Lenkung und Leitung des Polizeieinsatzes zu verzichten, sofern nicht im Einzelfall die Voraussetzungen der §§ 19a, 12a VersG vorliegen.

5. DVO-Meldegesetz (4.2, Drs S. 61 f)

Der Senat wird aufgefordert, bei der Schaffung von über den Grunddatenbestand hinausgehenden Zugriffsmöglichkeiten auf das Melderegister die Datenempfänger und die jeweiligen Einzeldaten präzise festzulegen.

6. Scheinanmeldungen verhindern durch Vorlage des Mietvertrages? (4.5, Drs S. 66 f)

Der Senat wird aufgefordert, im Rahmen der bundesgesetzlichen Novellierung des Melderechts dahingehend einzuwirken, dass Scheinanmeldungen unter Berücksichtigung der datenschutzrechtlichen Bestimmungen verhindert werden.

7. Beitreibung von Zahlungsrückständen durch Inkassobüros? (6.1, Drs. S. 77 ff)

Der Unterausschuss „Datenschutz und Informationsfreiheit“ regt an, dass der Datenschutzbeauftragte und das Bezirksamt Marzahn-Hellersdorf im Hinblick auf Forderungsvollstreckung/Inkasso/Factoring durch Dritte eine Empfehlung an den Senat und das Abgeordnetenhaus erarbeiten.

8. Gemeinsames Krebsregister (7.2.2, Drs S. 90 ff)

Der Senat wird aufgefordert sicherzustellen, dass die bei Kontrollen der technischen und organisatorischen Maßnahmen zum Datenschutz beim Gemeinsamen Krebsregister bereits 2009 festgestellten erheblichen Mängel und daraus resultierenden Risiken für die Vertraulichkeit der Registerdaten deutlich zügiger als bisher beseitigt werden. Dies gilt insbesondere für die Umstellung auf ein sicheres Meldeverfahren und die bisher noch nicht begonnene Erstellung und Umsetzung eines vollständigen Sicherheitskonzepts. Es setzt die Einstellung geschulten Personals für das Informationssicherheitsmanagement des Krebsregisters voraus.

9. Schwache Datenschutzorganisation in Klinikkonzernen (7.2.4, Drs S. 94 f)

Der Senat wird aufgefordert, darauf hinzuwirken, dass die seiner Aufsicht unterliegenden Krankenhausunternehmen - insbesondere der landeseigene Krankenhauskonzern Vivantes - den betrieblichen Datenschutz personell und sachlich angemessen ausstatten.

10. Auskunftsersuchen der Polizei gegenüber Krankenhäusern (7.2.6, Drs S. 98 f)

Der Senat wird aufgefordert, darauf hinzuwirken, dass die Krankenhäuser im Land Berlin jeweils eine zentrale Stelle bestimmen (z.B. Geschäftsleitung oder die ärztliche Direktion), die über das in der Regel schriftlich zu stellende Auskunftsersuchen der Polizei entscheidet. Auskunft darf nur erteilt werden, wenn dadurch im konkreten Fall eine gegenwärtige Gefahr für Leib, Leben oder persönliche Freiheit eines Menschen abgewendet werden kann. Auskunftsersuchen im Zusammenhang mit der Verfolgung von Straftätern aufgrund anderer Rechtsvorschriften bleiben unberührt.

11. Biographiedaten in der Pflege (7.2.7, Drs S. 99 ff)

Der Senat wird aufgefordert, die ambulanten und stationären Pflegeeinrichtungen im Land Berlin in geeigneter Weise darauf hinzuweisen, dass die Erhebung biografischer Angaben bei Pflegebedürftigen deren informierte Einwilligung voraussetzt und auf den für die Biografiearbeit erforderlichen Umfang zu beschränken ist.

12. Lehramtsanwärter auf Herz und Nieren geprüft (7.3.2, Drs S. 104 f)

Der Senat wird aufgefordert, ein Verfahren zu prüfen, dass Lehramtsanwärtern gestattet wird, dem Prüfungsamt zum Nachweis krankheitsbedingter Ausfallzeiten zunächst ein Attest vorzulegen, das nur eine Beschreibung der Symptome bzw. eine Darstellung der krankheitsbedingten Beeinträchtigungen sowie Angaben zu Beginn und voraussichtlicher Dauer der Erkrankung enthält. Erst wenn dieses Attest aufgrund der Art der beschriebenen Symptome im Einzelfall für die Feststellung der Prüfungsunfähigkeit nicht ausreicht, soll das Prüfungsamt ausnahmsweise die Vorlage eines substantiierten Attests mit Diagnose verlangen dürfen. Der Senat wird weiter aufgefordert, die Möglichkeit der Angleichung der Verfahren bei Krankheit der Prüfungsämter für Lehramtsanwärter und juristische Staatsexamina darzustellen und im Einvernehmen mit dem Datenschutzbeauftragten umzusetzen.

13. Behördliche Datenschutzbeauftragte an den Berliner Hochschulen (12.4.1, Drs S. 149 ff)

Der Senat wird aufgefordert, darauf hinzuwirken, dass die Hochschulen des Landes Berlin ihre behördlichen Datenschutzbeauftragten personell und sachlich angemessen ausstatten.

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 23. Juni 2011 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2009

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren,
mit dem **Jahresbericht** 2009 steht heute zum letzten Mal in dieser Wahlperiode ein Jahresbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Ihrer Tagesordnung. Dies nehme ich gerne zum Anlass, um Ihnen allen, insbesondere aber den Mitgliedern des Unterausschusses „Datenschutz und Informationsfreiheit" für die konstruktive Zusammenarbeit und Unterstützung in den zurückliegenden fünf Jahren zu danken.

Datenschutz und Informationsfreiheit haben in der Bundeshauptstadt einen hohen Stellenwert. Das liegt auch daran, dass das Parlament diesen beiden Grundrechten seit langem einen eigenen Unterausschuss widmet. Ich hoffe, dass auch das neu zu wählende Abgeordnetenhaus diese bewährte Übung fortsetzen wird. Denn in diesem Unterausschuss müssen Verwaltungen den Abgeordneten Rede und Antwort stehen, wenn sie es versäumt haben, ihre Praxis an den gesetzlichen Vorgaben zu orientieren. Das war auch im vergangenen Jahr der Fall und hat zu einer Reihe von Beschlussempfehlungen geführt, die Ihnen heute vorliegen. Sie behandeln eine große Bandbreite von praktisch bedeutsamen Fragen. Allein vier der dreizehn Beschlussempfehlungen betreffen den Gesundheitssektor, und das nicht ohne Grund.

Es gibt wohl kaum einen anderen Bereich des menschlichen Lebens, in dem so sensitive Informationen über den Einzelnen verarbeitet werden. Die Medizintechnik in Kliniken entwickelt sich rasant, ohne dass die Krankenhausinformationssysteme den Schutz des Patientengeheimnisses immer ausreichend gewährleisten würden. Wir haben deshalb auf Bund-Länder-Ebene unter Beteiligung der Krankenhäuser und der Hersteller die Erarbeitung einer Orientierungshilfe initiiert, die den Datenschutzbehörden jetzt bundesweit als Prüfmaßstab dient. Das ist ein wesentlicher Schritt hin zu einem pro-aktiv verstandenen Datenschutz. Denn es nützt den betroffenen Patienten wenig, wenn bei Prüfungen

nur festgestellt wird, dass in Krankenhäusern nicht nachvollzogen werden kann, wer wann auf ihre Daten zugegriffen hat, weil die technischen Systeme das bisher nicht protokollieren. Vielmehr sind jetzt auch die Hersteller solcher Systeme in die Pflicht genommen, ihren Teil dazu beizutragen, damit datenschutzgerechte Technik auf den Markt kommt, die die Einhaltung der ärztlichen Schweigepflicht in einem hochtechnisierten Klinikumfeld erst ermöglicht.

Allerdings ist unverständlich, dass ein landeseigenes Unternehmen wie Vivantes – immerhin der größte kommunale Krankenhauskonzern Deutschlands – meint, es genüge ein einziger Datenschutzbeauftragter für das gesamte Unternehmen. Dieser Konzern, der im vergangenen Jahr sechs Millionen Euro Gewinn gemacht hat, ist bekanntlich aus den ehemaligen Krankenhäusern der Bezirke gebildet worden, die jeweils eigene Datenschutzbeauftragte hatten. Wenn man das Beispiel der Charité zugrundelegt, müsste auch bei Vivantes pro 1000 Betten ein Datenschutzbeauftragter bestellt werden, um die gesetzlichen Aufgaben auch nur halbwegs erfüllen zu können. Hier ist der Senat aufgefordert, seinen Einfluss auf das Unternehmen entsprechend geltend zu machen.

Aber auch der gesetzliche Rahmen für den Datenschutz in Berliner Krankenhäusern muss neu bestimmt werden. Hierzu wird in den Ausschüssen des Abgeordnetenhauses gegenwärtig ein Gesetzentwurf des Senats zur **Neuregelung des Krankenhausrechts** beraten, der wichtige Klarstellungen zum Datenschutz in einer hochtechnisierten Klinikumgebung enthält und in enger Abstimmung mit uns formuliert worden ist. Gegenüber dem federführenden Ausschuss habe ich einen zusätzlichen Vorschlag zur Klarstellung gemacht, der verbleibende Einwände ausräumen sollte. Ich appelliere an Sie, diesen Gesetzentwurf – zumindest aber die darin enthaltenen überfälligen Neuregelungen des Datenschutzes – noch vor dem Ende der Legislaturperiode zu beschließen. Die Krankenhäuser in der Bundeshauptstadt benötigen endlich Rechtssicherheit, wenn sie sich auf ihr Kerngeschäft konzentrieren und Patientendaten im Rahmen des Outsourcings für bestimmte Zwecke an externe Unternehmen weitergeben.

Im Bereich der **Informationsfreiheit** hat Berlin im vergangenen Jahr erhebliche Fortschritte gemacht. Das ist zum einen auf die vom Abgeordnetenhaus beschlossene Änderung des Informationsfreiheitsgesetzes, aber auch auf den Volksentscheid vom Februar dieses Jahres zurückzuführen. Ich denke, es ist kein

Zufall, dass der erste erfolgreiche Volksentscheid in Berlin Fragen der Informationsfreiheit betraf. In diesem Zusammenhang begrüße ich es auch sehr, dass das Abgeordnetenhaus den widerwilligen Senat aufgefordert hat, externe Beratungsleistungen bei Gesetzentwürfen (sog. Footprints) namhaft zu machen.

Aber sowohl beim Datenschutz wie auch bei der Informationsfreiheit gibt es keinen Grund, sich zufrieden zurückzulehnen. Die Herausforderungen in beiden Bereichen nehmen zu, das machen die Schlagzeilen in den Medien nahezu täglich deutlich. Es reicht dabei auch nicht, auf die Zuständigkeit des Bundes zu verweisen. Berlin wirkt über den Bundesrat an der Bundesgesetzgebung mit. Deshalb ist es erfreulich, dass der Senat in der vergangenen Woche meine Anregung aufgegriffen und eine Entschließung des Bundesrats herbeigeführt hat, in der die Bundesregierung aufgefordert wird, bei der Energiewende und insbesondere beim **Aufbau intelligenter Energieversorgungsnetze** den Datenschutz stärker zu berücksichtigen.

Der Bildungssenator hat 2011 zum „Jahr der Medienkompetenz“ erklärt. Es kann kein Zweifel daran bestehen, dass die Anstrengungen zur Steigerung der Medienkompetenz und damit auch des Datenschutz-Bewusstseins in den Berliner Schulen erhöht werden müssen. Umso befremdlicher ist es, dass die Bildungsverwaltung neuerdings einen **Facebook-Auftritt** hat. Dieses Unternehmen ist international bekannt für seine Geringschätzung des Datenschutzes. Demgegenüber bietet ein Berliner Unternehmen soziale Netzwerke wie SchülerVZ oder StudiVZ an, die wesentlich datenschutzfreundlicher sind. Mir ist unerklärlich, weshalb nicht ausschließlich solche Angebote genutzt werden. Entweder hat man sich in der Bildungsverwaltung bewusst für einen Massentrend und gegen den Datenschutz entschieden, oder die linke Hand weiß dort nicht, was die rechte tut.

Meine Damen und Herren,
Sie haben mich zur Wahrung der Rechte auf informationelle Selbstbestimmung und auf Informationszugang in dieses Amt gewählt. Datenschutz und Informationsfreiheit sind Grundrechte, deren Wahrung nicht allein Aufgabe eines Beauftragten und seiner Mitarbeiter ist. Vielmehr hoffe ich dabei auch künftig auf Ihre nachhaltige Unterstützung.

Herzlichen Dank für Ihre Aufmerksamkeit.

Stichwortverzeichnis

F

G

H

I

J / K

L

M / N

O

P

Q / R

S

T

U / V

W

Z

Veröffentlichungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte:
Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über seine Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. Der Tätigkeitsbericht wird von uns auch als Broschüre für die Bürgerinnen und Bürger veröffentlicht.

Dokumente zu Datenschutz und Informationsfreiheit:
Diese Schriftenreihe erscheint jährlich als Anlage zu unserem Tätigkeitsbericht. Sie enthält die bedeutsamen Dokumente der nationalen und internationalen Arbeitsgruppen und Konferenzen des genannten Jahres.

Berliner Informationsgesetzbuch (BlnInfGB):
In dieser Textsammlung werden von uns die wichtigsten Regelungen zum Datenschutz und zur Informationsfreiheit für das Land Berlin herausgegeben.

Ratgeber und Faltblätter zum Datenschutz:
In diesen Publikationen haben wir praktische Informationen zu einzelnen Fragen im Alltag zusammengestellt. Damit wollen wir die Menschen in die Lage versetzen, ihre Datenschutzrechte bzw. ihr Recht auf Informationszugang eigenständig wahrzunehmen.

Welche Broschüren wir im Einzelnen veröffentlicht haben, können Sie einer Übersicht auf unserer Website www.datenschutz-berlin.de entnehmen. Den überwiegenden Teil unserer Broschüren haben wir dort für Sie auch zum Download bereitgestellt. Eine Bestellung per Post ist gegen Einsendung eines an Sie selbst adressierten und mit 0,85 Euro frankierten DIN-A5-Umschlages möglich.

www.datenschutz-berlin.de

Verwaltungsmodernisierung • Aktuelle Datenschutzgesetzgebung in Berlin • **Liquid Democracy** • Landeskrankenhausgesetz • Cloud Computing • **Justizvollzugsdatenschutzgesetz** • Novellierung des Berliner Datenschutzgesetzes • **Soziale Netzwerke** • Videoüberwachung der Intimsphäre • Touch & Travel • Einführung der elektronischen Fußfessel • **Patientenbefragung** durch das Finanzamt • Gerichtsvollzieher arbeiten nicht für das Jugendamt • Orientierungshilfe **Krankenhausinformationssysteme** • Smart Metering: Wie intelligent dürfen **Stromzähler** werden? • Das Jahr des **„Zensus 2011“** • Umsetzung des Bildungs- und Teilhabepakets (BuT) • Datenschutzmängel bei Markt- und Meinungsforschungsinstitut • Datenschutz-Kodex für Geodatendienste • **Datenlecks** bei öffentlichen und privaten Stellen • Anonyme Bezahlverfahren • **BVV-Sitzungen im Internet** • Gebühren im Bauaktenarchiv