Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Datenschutz und Informationsfreiheit

Bericht 2010

Berlin

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2010

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 **31. März 2010** vorgelegten Jahresbericht 2009 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2010 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2010“) veröffentlicht.

Dieser Jahresbericht ist über das Internet (www.datenschutz-berlin.de) abrufbar.

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4-10, 10787 Berlin
Telefon: (0 30) +138 89-0
Telefax: (0 30) 215 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: www.datenschutz-berlin.de

Satz: LayoutManufaktur.com
Druck: Offsetdruckerei Holga Wende

Inhaltsverzeichnis

Einleitung

Datenschutz und Informationsfreiheit waren im zurückliegenden Jahr so häufig Gegenstand der öffentlichen Debatte wie seit der Volkszählung 1987 in der alten Bundesrepublik nicht mehr. Das war gut so und hatte mehrere Gründe, die sich mit den Stichworten Google Street View, Vorratsdatenspeicherung, unabhängige Datenschutzkontrolle und Wikileaks umschreiben lassen. Diese Diskussionen hatten naturgemäß auch Auswirkungen auf die Tätigkeit des Beauftragten für Datenschutz und Informationsfreiheit in Berlin.

Die Debatte über den Online-Panoramadienst **Google Street View** setzte in der Bundeshauptstadt erst ein, lange nachdem die Fahrzeuge des US-Unternehmens ihre Aufnahmen gemacht hatten. Als Google auf Druck der zuständigen Hamburger Aufsichtsbehörde allen Menschen in Deutschland ein Recht zum Vorabwiderspruch gegen die Veröffentlichung ihrer Häuser und Wohnungen eingeräumt hatte, machten allein in den ersten zwanzig deutschen Städten, die man bundesweit virtuell besuchen konnte (darunter auch Berlin), rund 255.000 Personen von dieser Möglichkeit Gebrauch.[1] Damit wurde erstmals ein Grundsatz zum Umgang mit Gebäudebild-Datenbanken praktisch umgesetzt, den die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) bereits 1999 formuliert hatte.[2]

Teilweise wurde die – europaweit geführte – Debatte über Google Street View als verfehlt bezeichnet. Das ist nur insofern zutreffend, als es bei Street View nicht um einen Eingriff in die Privatsphäre der Menschen geht. **Datenschutz reicht aber über den Schutz der Privatsphäre hinaus.** Er betrifft – in einer unglücklich verknappten Formulierung – den Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten.[3] Gerade darum geht es auch bei Google Street View: Ein Unternehmen wollte personenbezogene Daten in eine weltweit verfügbare Datenbank einstellen, ohne die Betroffenen in irgendeiner Weise zu beteiligen. Hinzu kam, dass Google erst auf Nach-

1 Vgl. 1.1.2
2 Vgl. Dokumentenband 1999, S. 29 ff.
3 So der treffende Titel der Konvention Nr. 108 des Europarats vom 28. Januar 1981

frage der Aufsichtsbehörde einräumte, es seien von den Kamerawagen auch die Daten von privaten WLAN-Zugängen und – wie das Unternehmen angab – unabsichtlich auch Inhaltsdaten wie E-Mails oder Passwörter erfasst worden. Auch die bildliche Darstellung von Häusern und Mietwohnungen gibt Auskunft über die Verhältnisse ihrer Bewohner. Dabei handelt es sich zwar bisher nur um Standbilder, die schnell veralten. Aber schon jetzt können Häuser, Hinterhöfe und Gärten aus der Vogelperspektive („bird's view") und aus dem Weltall betrachtet werden, und bei Standbildern wird es nicht bleiben: Es ist nur eine Frage der Zeit, dass **Live-Aufnahmen** gemacht und veröffentlicht werden.

Die Kameras werden näher kommen, soviel ist sicher. Street View ist nur ein erster, harmlos erscheinender Schritt in einer Entwicklung. Deshalb war und ist die öffentliche Diskussion darüber wichtig. Etwas anderes kommt hinzu: 2007 berichtete der Google-Manager Andy McLaughlin[4] auf einer Konferenz in den USA, die US-Regierung habe das Unternehmen gefragt, ob es in der Lage sei, alle privaten Videokameras in den USA so zu vernetzen, dass staatliche Behörden jederzeit auf sie zugreifen können. Google habe geantwortet, das sei technisch möglich, man werde einer solchen Forderung aber aus gesellschaftlichen und ethischen Gründen nicht Folge leisten. Aus den gleichen Gründen hat dasselbe Unternehmen es bisher abgelehnt, die bereits vorhandene Software „Goggles"[5], mit der Gebäude und online gespeicherte Bilder von Personen identifiziert werden können, nicht zur **Gesichtserkennung** auf Smartphones in Echtzeit verwenden zu wollen. Ob Technologien wie die Live-Rundumüberwachung oder Gesichtserkennung Privatpersonen oder Behörden zur Verfügung gestellt werden, sollte aber nicht den jeweiligen Unternehmensvorständen überlassen bleiben.

Das Bundesverfassungsgericht hat in seinem **Urteil zur Vorratsdatenspeicherung** betont, dass der Schutz vor lückenloser Überwachung zur deutschen Verfassungsidentität gehöre, die selbst im europäischen Einigungsprozess nicht aufgegeben werden dürfe.[6] Das ist nicht nur auf die Bevorratung von Verkehrsdaten der Telekommunikation, sondern auch auf die visuelle Überwachung und die zentrale Speicherung von Beschäftigtendaten im **ELENA-Verfahren**[7] zu beziehen. Aus demselben Grund muss die Bundesregierung auch Plänen der Europäischen Kommission eine Absage erteilen, die nach dem Ende des Berichtszeitraums bekannt wurden: Danach sollen Daten von **Flugpassagieren**, die aus Drittstaaten nach Europa reisen oder Europa in umgekehrter Richtung verlassen, auf Vorrat für fünf Jahre anlasslos gespeichert werden und für eine jederzeitige Rasterfahndung zur Verfügung stehen.

Die Debatte über die vom Bundesverfassungsgericht nicht völlig ausgeschlossene Vorratsspeicherung bei Verkehrsdaten der Telekommunikation ist noch nicht abgeschlossen, zumal die Evaluation der europäischen Richtlinie zu diesem Thema noch aussteht.[8] Unverständlich ist allerdings, dass die Bundesregierung die beim Bundeskriminalamt angeblich vorliegenden Erkenntnisse über den Nutzen der anlasslosen Speicherung von Verkehrsdaten der Telekommunikation nach wie vor unter Verschluss hält.[9] Zudem ist schon seit geraumer Zeit festzustellen, dass die Vorratsdatenspeicherung, die auf europäischer Ebene ursprünglich als Reaktion auf die Terroranschläge in Madrid und London durchgesetzt wurde, von ihren Befürwortern jetzt als unbedingt notwendig zur Bekämpfung bestimmter Formen der Telefon- und Internet-Kriminalität (vom „Enkeltrick" bis zur Kinderpornographie) angesehen wird. Das macht das Ausmaß der schleichenden Zweckentfremdung deutlich, noch bevor der Bundesgesetzgeber überhaupt über eine verfassungskonforme Neuregelung entschieden hat. Zudem haben die Sicherheitsbehörden auch ohne Vorratsdatenspeicherung beachtliche Erfolge erzielt.

Eine deutliche **Stärkung der unabhängigen Kontrolle des Datenschutzes** hat der Europäische Gerichtshof mit seiner Entscheidung gegen die Bundesrepublik Deutschland bewirkt.[10] Er hat die Auffassung der Datenschutzbeauftragten in Bund und Ländern bestätigt, dass die gegenwärtige Organisation der Datenschutzaufsicht für die Wirtschaft nicht mit den Vorgaben der EU-Richtlinie zum Datenschutz vereinbar ist. Zugleich hat der Gerichtshof betont, dass die Unabhängigkeit der Datenschutzaufsichtsbehörden eingeführt wurde, *„um*

4 McLaughlin war später (Mai 2009 – Dezember 2010) stellvertretender Chief Technology Officer im Stab von Präsident Obama.
5 Englischer Begriff (ugs.) für „Brille"
6 Urteil vom 2. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833, 839 f., Rn. 218;Vgl. 13.1
7 Vgl. 2.3
8 Vgl. 13.1
9 Vgl. Antwort der Bundesregierung vom 29. November 2010 auf die Kleine Anfrage der Abgeordneten Korte u. a., BT-Drs. 17/3974
10 Urteil vom 9. März 2010, Rechtssache C-518/07, NJW 2010,1265 ff.

die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen oder ihren Bevollmächtigten eine besondere Stellung zu verleihen"[11]. Im Berichtszeitraum wurde die notwendige Anpassung des Berliner Datenschutzgesetzes an die Rechtsprechung des Europäischen Gerichtshofs noch nicht vorgenommen; allerdings hat der Senat einen entsprechenden Gesetzentwurf dem Abgeordnetenhaus zugeleitet.

Gleichzeitig gibt es allerdings Anzeichen dafür, dass das Konzept der **Datenschutzaufsicht im föderalen System** in Frage gestellt wird. Bundesgesetze werden nach der Verfassung von den Ländern ausgeführt. Deshalb ist die Kontrolle der damit verbundenen Verarbeitung von Bürgerdaten und die Aufsicht über den Datenschutz in der Wirtschaft nach dem Bundesdatenschutzgesetz seit jeher den Datenschutzbeauftragten und Aufsichtsbehörden der Länder zugewiesen. Diese koordinieren ständig ihr Vorgehen untereinander und mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Das System der Datenschutzkontrolle im Bundesstaat hat sich gerade auch im Umgang mit international agierenden Unternehmen durchaus bewährt. Nun hat der Bundesgesetzgeber im Zuge der Reform der sog. Hartz IV-Gesetze[12] nicht nur der Bundesagentur für Arbeit praktisch die Funktion eines „Bundessozialamtes" zugewiesen.[13] Damit aber nicht genug: Während nach der bisherigen Rechtslage die Landesdatenschutzbeauftragten die Datenverarbeitung in den Jobcentern zu kontrollieren hatten und dies auch in Berlin mit gutem Erfolg geschehen ist[14], wird ab dem 1. Januar 2011 allein der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hierfür zuständig sein. Das bedeutet einen erheblichen Verlust an Bürgernähe, denn der Bundesbeauftragte wird auf Beschwerden naturgemäß nicht in der Promptheit reagieren können, wie dies die Landesdatenschutzbeauftragten bisher getan haben.

Auch die gerade erst begonnene Diskussion über die geplante **Stiftung Datenschutz**[15] ist in diesem Zusammenhang bedeutsam. Gerade weil es sich dabei um eine Bundesstiftung handeln soll, kommt es entscheidend darauf an, dass sie die Zuständigkeit der Datenschutzbeauftragten und Aufsichtsbehörden der Länder beachtet und mit diesen eng zusammenarbeitet.[16] Vor allem im wichtigen Bereich der Medienkompetenz ist die ausschließliche Zuständigkeit der Länder im Bildungsbereich zu wahren.

Insgesamt muss die schon zu lange verschleppte grundlegende Modernisierung des Datenschutzrechts jetzt aber auf europäischer und internationaler Ebene vorangetrieben werden. Das von der Kommission vorgelegte **Gesamtkonzept für den Datenschutz in der Europäischen Union**[17] bietet eine geeignete Grundlage für die Formulierung eines europäischen Datenschutzgesetzes. Dabei ist es angesichts der immensen Datensammlungen bei Unternehmen wie Google, Facebook und Apple dringend erforderlich, die Anwendbarkeit europäischen Datenschutzrechts auf solche Unternehmen eindeutig klarzustellen. Wenn ein Berliner Unternehmen Geschäfte auf dem US-amerikanischen Markt macht, stellt niemand in Frage, dass es sich an das in den Vereinigten Staaten geltende Recht zu halten hat. Entsprechendes hat für US-Unternehmen zu gelten, die auf dem europäischen Markt tätig sind. Zudem darf der neue europäische Rechtsrahmen nicht zum kleinsten gemeinsamen Nenner werden, sondern muss das bereits erreichte Datenschutzniveau gerade angesichts der Rolle des Internets ausbauen.

Die Veröffentlichung von zahlreichen Depeschen US-amerikanischer Diplomaten durch **Wikileaks** hat sowohl ein Schlaglicht auf Fragen des Datenschutzes als auch der Informationsfreiheit geworfen. Bezeichnenderweise hatte die US-Regierung nach dem 11. September 2001 aufgrund angeblicher Kommunikationsmängel zur Erhöhung der Sicherheit 2,5 Millionen Personen den Zugriff auf das Regierungsnetz SPRnet eröffnet, aus dem die jetzt veröffentlichten Depeschen stammten. Das zeigt, dass Maßnahmen zur Terrorismusbekämpfung, die eigentlich sicherheitserhöhend wirken sollen, den gegenteiligen Effekt jedenfalls auf die Informationssicherheit haben können.

11 Ebenda, S. 1266
12 § 50 Abs. 4 Satz 3 SGB II, eingefügt durch das Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitsuchende, BGBl. 2010 I, S. 1112, 1121
13 Dabei bleiben hier die sog. Optionskommunen in den Flächenländern und die Übernahme der Unterkunftskosten, die nicht in die Bundeszuständigkeit fällt, außer Betracht.
14 Vgl. JB 2005, 3.2; JB 2006, 5.1.1; JB 2007, 7.2.1; JB 2008, 8.1.2; JB 2009, 7.1.1
15 Vgl. 12.1
16 Vgl. Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Förderung des Datenschutzes durch Bundesstiftung, Dokumentenband 2010, S.21
17 Vgl. 11.1

Aufschlussreich für den Datenschutz war auch eine Folgeerscheinung der Wikileaks-Veröffentlichungen: Deren Urheber hatten die umfangreichen Dokumente auf den Servern des Unternehmens Amazon in einer „Cloud“ gespeichert. Nach Medienberichten beendete das Unternehmen aufgrund des Anrufs eines US-Senators, der über das Vorgehen von Wikileaks empört war, einseitig die Vereinbarung mit Wikileaks. Die Daten waren vorübergehend nicht verfügbar. Das macht schlaglichtartig das Risiko des Kontrollverlustes deutlich, das mit vielen Formen des Cloud Computing stets verbunden ist.[18]

Die Grundfrage bei Wikileaks betrifft aber die Legitimität der Veröffentlichungen selbst. Diese Frage ist differenziert zu beurteilen. Soweit Wikileaks Videoaufnahmen über Luftangriffe auf Zivilisten im Irak („collateral murder“) publiziert hat, war dies gerechtfertigt. Bei anderen Veröffentlichungen ist dies weniger eindeutig. Es gibt gerade auch im diplomatischen Verkehr, aber nicht nur dort, vertrauliche Informationen, deren Schutz Vorrang vor dem öffentlichen Informationsinteresse haben sollte. Auch ist nicht klar, ob Wikileaks genug zum Schutz von Informanten und Gewährspersonen getan hat. Vor allem zu kritisieren ist die Tatsache, dass Wikileaks die Abwägung zwischen den Informationsinteressen der Öffentlichkeit und dem Geheimhaltungsbedürfnis Einzelner nach intransparenten und deshalb nicht überprüfbaren Maßstäben vornimmt. Diese Abwägung sollte im Rahmen der – durchaus verbesserungsbedürftigen – Informationsfreiheitsgesetze nach allgemein verbindlichen und kontrollierten Kriterien vorgenommen und nicht einer privaten Organisation überlassen werden.

Andererseits dürfen die Wikileaks-Veröffentlichungen nicht zum Vorwand genommen werden, um von staatlicher Seite Informationen, an denen ein unbestreitbares öffentliches Interesse besteht, in unzulässiger Weise unter Verschluss zu halten oder die Informationsfreiheit generell wieder einzuschränken.[19] Das Bundesverfassungsgericht hat am Beispiel des Gentechnikgesetzes deutlich gemacht, das auch öffentlich zugängliche personenbezogene Register – in diesem Zusammenhang das Standortregister über Freisetzungen und Anbau gentechnisch veränderter Organismen – innerhalb der demokratischen, pluralistischen Gesellschaft einen wichtigen Beitrag zum öffentlichen Meinungsbildungsprozess leisten.[20] Das gilt in gleicher Weise für zahlreiche andere staatliche Register und Datensammlungen, soweit die legitimen Geheimhaltungsinteressen dort verzeichneter Personen berücksichtigt werden.

18 Vgl. JB 2008, 1.1.1

19 Vgl. dazu die Entschließung der Konferenz der Informationsfreiheitbeauftragten in Deutschland vom 13. Dezember 2010: Open Data: Mehr statt weniger Transparenz!, Dokumentenband 2010, S. 169

20 BVerfG, Urteil vom 24. November 2010 – 1 BvF 2/05, Rn. 175

1. Technische Rahmenbedingungen

1.1 Entwicklung der Informationstechnik

1.1.1 Nach A-, B- und C- jetzt auch D(igitale)-Kriegsführung?

Die heutige Informationsgesellschaft hängt auf Gedeih und Verderb vom Funktionieren der weltweiten informationstechnischen Infrastrukturen ab. Die auf der Welt kursierenden Finanzgüter sind elektronisches Geld, das per Mausklick in Sekundenbruchteilen zwischen Metropolen und Staaten hin und her transferiert wird. Die konzerninterne Kommunikation, die Kommunikation zwischen den Marktteilnehmern, der elektronische Handel werden über das Internet geführt. Die Nachrichten über Ereignisse sind Sekunden nach ihrem Eintritt für alle im Internet abrufbar. Über das Internet als Träger der Smart Grids[21] wird künftig die Erzeugung und Verteilung elektrischer Energie in Abhängigkeit vom Verbrauchsverhalten der Stromabnehmenden gesteuert. Ohne das Internet, seine Server, seine Netzkomponenten, seine Leitungen, die Millionen Server der Teilnehmenden aus Wirtschaft, Politik und Verwaltung und die Abermillionen Computer der Internetkonsumenten hätten wir keine Informationsgesellschaft, die gesellschaftlichen Prozesse wären mit den heutigen nicht vergleichbar.

Das Internet hat sich chaotisch entwickelt. Aus einem erfolgreichen, Ende der 60er Jahre des 20. Jahrhunderts beginnenden militärischen, bald darauf auch wissenschaftlichen Experiment, Rechner mit unterschiedlichen Betriebssystemen mithilfe paketvermittelnder Protokolle miteinander Daten austauschen zu lassen, wurden bald E-Mail-Dienste entwickelt, später dann das World Wide Web erfunden. Zunächst war das Internet den Insidern und Experimentierern vorbehalten. Es war ergänzende Informationsquelle und wurde von einer versuchsfreudigen Community nach ihren Regeln und den Marktgesetzen weiter entwickelt. Die Frage nach **Sicherheit im Internet** stellte sich nur den üblichen Bedenkenträgern.

21 Vgl. JB 2009, 1.1.1

Dagegen ist Informationssicherheit heute ein boomendes Fachgebiet der Informatik, aber auch ein vergleichbar neues. In der Geschichte der Informatik kam die Sicherheit in der Datenverarbeitung erst spät vor, möglicherweise zu spät, denn die Versäumnisse der Vergangenheit lassen sich nicht vollständig aufholen. Als Mitte der 80er Jahre des vergangenen Jahrhunderts Computerviren und ihre Bedrohungen bekannt wurden, waren viele Kernstrukturen moderner Standardsoftware, insbesondere der Betriebssysteme, längst entwickelt. Die inzwischen ergänzten Sicherheitsfeatures sind keine Bestandteile des Systemdesigns, sondern nachträgliche Reparaturen.

Alle anderen wesentlichen Technologien – die Bautechnologie, die Verkehrstechnologien für Straße, Schiene und Luft, die Elektrotechnik – haben strenge und streng kontrollierte Regelwerke, die die Sicherheit ihrer Produkte betreffen. Sicherheit war bei ihnen von Anfang an Triebfeder der Entwicklung. Dies kann allerdings aus oben angedeuteten Gründen von der Softwaretechnologie nicht behauptet werden. Angriffe auf IT-Systeme geschehen täglich milliardenfach, die meisten werden von den inzwischen entwickelten Schutztechniken abgewehrt, weil selbst der einfache Familienhaushalt für seinen PC oder sein Notebook Antiviren- und Firewallschutz einsetzt. Viele Angriffe zeigen keine Wirkung, weil die erfolgreich angegriffenen Rechner nicht zum Feindschema passen. Dennoch gibt es dauernd Schlagzeilen zu spektakulären Sicherheitsverletzungen, bedingt durch grobe Fahrlässigkeit der Opfer oder durch die geschickte Nutzung von Sicherheitslücken, die weltweite Standardsoftwareprodukte nach wie vor aufweisen.

Wer 2,5 Millionen Menschen Zugang zu vertraulichen Daten der amerikanischen Diplomatie ermöglicht, muss sich nicht wundern, wenn **Wikileaks** bald zur „Zweitveröffentlichung“ startet. Der im Herbst wirkende **Stuxnet-Wurm,** auf den wir später zurückkommen, war ein Beispiel für die aufwändige und geschickte Nutzung von zum Teil bisher unbekannten Sicherheitslücken von Standardsoftware. Für solche Sicherheitslücken, sog. Zero-Day-Exploits, grassiert ein lukrativer Schattenhandel.

Beim Wettbewerb zur Suche des Wortes 2010 wurde der Begriff **„Cyberkrieg“** auf den vierten Platz gesetzt. Dies macht deutlich, dass zumindest für die Opfer spektakuläre Sicherheitsvorfälle im Internet die Dimension kriegerischen Handelns erhalten haben. Die Tatsache, dass Informationstechnik zum

Mittel und Ziel kriegsähnlicher Handlungen werden kann, ist ein dunkler Aspekt der Entwicklung der Informationstechnologie. Zugleich bedroht diese Entwicklung die Verfügbarkeit personenbezogener Daten, die heute fast nur noch mit informationstechnischen Systemen verarbeitet werden. Umgekehrt können Maßnahmen gegen Cyberattacken zu exzessiver Überwachung des Internet-Verkehrs führen.

Bereits 1995 wurde unter dem Begriff „Cyber-Terrorismus" die Bedrohung von DV-Zentralen durch Formen der elektronischen Kriegsführung diskutiert[22]. Dabei ging es aber noch nicht um Softwareangriffe, sondern um Angriffe auf informationstechnische Infrastrukturen mithilfe von elektronischen Bomben, mit denen hochenergetische Radiowellen punktgenau oder starke elektromagnetische Impulse ungerichtet ausgestrahlt werden können, die Infrastrukturen stören oder zerstören können. Solche Szenarien waren damals Gegenstand einer amerikanischen Konferenz zur „Information-Warfare". Auch wenn diese Form der Angriffe nichts mit den späteren Softwareattacken zu tun hatte, das Ziel war damals wie heute das gleiche: Die Ausschaltung oder zumindest Schwächung gegnerischer informationstechnischer Infrastrukturen.

Nach dem 11. September 2001 wurde erneut die Aufmerksamkeit darauf gelegt, dass neben den damaligen Terrorattacken mit physischer Gewalt auch Cyberattacken zu befürchten seien, speziell durch Hacking und Virenbefall von Börsencomputern, Stromversorgern, Notfallzentralen, Militäreinrichtungen und Telefonzentralen. Die Gefahr war umso greifbarer, als die Informationssicherheit dieser Einrichtungen nach Untersuchungen von Sicherheitsexperten unzureichend war[23].

Im April 2007 wurden nach einer politischen Aktion, die in Russland als Provokation empfunden wurde, Server der estnischen Regierung, estnischer Banken und anderer Unternehmen des Landes durch Dedicated Denial of Service-Angriffe (DDoS) blockiert. Dabei werden die angegriffenen Server gezielt mit massenhaften Anfragen innerhalb kurzer Zeit durch Zusammenwirken Tausender von Rechnern überflutet, damit sie an Überlast zusammenbrechen. Daraus hat die estnische Regierung zunächst Vorwürfe abgeleitet, wonach Russland für diese Angriffe verantwortlich sei. Zum ersten Mal überhaupt war damit ein unabhängiger Staat Ziel solcher Angriffe aus dem Internet gewesen. Die estnische Regierung schaltete EU und NATO ein und erwog, dass in solchen Fällen der Verteidigungsfall in der Nato ausgerufen werden müsse[24]. Experten kamen später zu dem Ergebnis, dass der Angriff über weltweite Botnetze geführt wurde, die möglicherweise von russischen Nationalisten initiiert wurden, jedoch nicht vom russischen Staat.

„Das Phantom des Cyberwar" wurde 2008 von der „tageszeitung" illustriert[25]. Der Artikel berichtete über diverse Ereignisse, die von Repräsentanten der angegriffenen Staaten zunächst als Angriffe auf kritische Infrastrukturen ihres Staates öffentlich als feindliche Handlungen beklagt und von den vermuteten Aggressoren entweder prompt dementiert wurden oder unkommentiert blieben:

- Anzeichen einer russischen Computerattacke auf Georgien, für die zu Beginn des Kaukasus-Kriegs ein russisches Business Network verantwortlich sein sollte;
- nach Angaben eines US-Abgeordneten das Eindringen chinesischer Hacker auf der Suche nach Dissidentenlisten in mehrere Rechner des Kongresses;
- nach Angaben der CIA im Januar 2008 das Eindringen von angeblichen Cyber-Terroristen bei Stromversorgern außerhalb der USA mit der Folge von Stromausfällen;
- das US-Verteidigungsministerium teilt im Mai 2008 dem Geheimausschuss mit, das Rechnernetz des Ministeriums werde täglich mehr als 300 Millionen Mal von außerhalb gescannt und angegriffen;
- zur gleichen Zeit unterrichtete der deutsche Verfassungsschutz das Bundeskanzleramt und die Staatssekretäre des Innen-, Außen-, Justiz- und Verteidigungsministeriums von einem Computerangriff, der vermutlich von der chinesischen Volksbefreiungsarmee kam.

22 „Unternehmens-DV durch Cyberterroristen bedroht", Computerwoche vom 10. März 1995, S. 41

23 „Wir halten die Augen offen", Der Tagesspiegel vom 16. September 2001, S. 31; „Attacken aus dem Laptop", Süddeutsche Zeitung vom 15. Oktober 2001, S. 2; „US-Experte warnt vor Terror im Cyberspace", Berliner Morgenpost vom 4. Januar 2002, S. 21

24 heise online vom 12. Juni 2007

25 taz.de am 11. August 2008

Es gilt allerdings als offenes Geheimnis, dass Hacker von Staaten dafür ausgebildet werden, um im Ernstfall digitale Angriffe auf wichtige Infrastrukturen auszuführen. Dagegen wappnen sich die Zielstaaten. So gibt es in den USA die „United States Cyber Command", eine Behörde, welche zur Aufgabe hat, die Sicherheit der Computersysteme des Landes zu verteidigen. In Deutschland gibt es seit 1998 eine interministerielle **Arbeitsgruppe zum Schutz kritischer Infrastrukturen (KRITIS)**.

Der Verdacht, dass digitale Kriegshandlungen bei offenkundig politisch motivierten Angriffen auf Einrichtungen eines souveränen Staates vorliegen könnten, kam in jüngster Zeit auf, nachdem Meldungen von Störungen in Anlagen des iranischen Atomprogramms bekannt wurden, die auf das Wirken einer besonders aufwändigen und raffinierten Schadsoftware zurückzuführen waren.

Seit Mitte September berichten die Medien über ein Computerschadprogramm namens **„Stuxnet"**[26]. Die Europäische Agentur für Internetsicherheit (ENISA) spricht im Zusammenhang mit den Angriffen des Stuxnet-Wurms von einem Paradigmenwechsel hinsichtlich gezielter Angriffe gegen kritische Infrastrukturen. Sie warnt vor ähnlichen Attacken in der nahen Zukunft. „Die Angreifer haben viel Zeit und Geld investiert, um ein derartiges gefährliches Tool zu entwickeln. Die Tatsache, dass Täter dieses Tool aktiviert haben, kann als ein „erster Schlag" angesehen werden", stellt der geschäftsführende Direktor der ENISA, Dr. Udo Helmbrecht, fest[27].

Stuxnet ist ein im Juli erstmals entdeckter Computerwurm und gilt unter Computerexperten als **das bis dato komplexeste Stück Schadprogramm**, das nahezu alle bisher bekannten Angriffsformen vereint. Daher vermutet die Fachwelt, dass es sich um den Probelauf eines staatlich organisierten Angriffes bzw. einer kriminellen Vereinigung handelt. Sein Ziel ist es offenbar, Steuerungssysteme in Industrieanlagen auf Basis von Siemens-Produkten zu stören, wobei diese nicht nur ausspioniert, sondern auch deren Funktionsweisen manipuliert werden. Seine Arbeitsweise und Verbreitungswege sind weitgehend aufgeklärt.

26 Z. B. „Siemens meldet Hackerangriff auf Industrieanlagen", Die Welt vom 18. September 2010, S. 11; „Der digitale Erstschlag ist erfolgt", Frankfurter Allgemeine Zeitung vom 22. September 2010, S. 33

27 c´t vom 25. Oktober 2010, S. 43

Stuxnet nutzte verschiedene Schwachstellen, **gestohlene digitale Signaturen** und bis daher unbekannte Sicherheitslücken des Betriebssystems Windows (**sog. Zero-Day-Exploits**), um sich in Windows-Systemen zu verbreiten. Nach dem Befall suchte der Wurm nach einem bestimmten Programm der Fa. Siemens, welches der Überwachung und Steuerung technischer Prozesse dient. Wenn er außerdem eine bestimmte Siemens-Software zur Programmierung der Steuerung von Maschinen und Anlagen fand, tauschte er spezielle Dateien aus, um etwa Sollwerte für die Steuerung von Anlagen zu manipulieren.

Entdeckt wurde das Auftreten von Stuxnet durch die bekannt gewordenen Angriffe auf Anlagen des iranischen Atomprogramms, die mit der beschriebenen Siemens-Software bestückt waren. Der stellvertretende Leiter der iranischen IT-Organisation sagte der Presse, der Kampf gegen die Stuxnet-Attacke im Iran sei noch lange nicht beendet, da der Virus konstant aktualisiert werde[28].

Nach Angaben von Siemens hat der Stuxnet-Wurm neben Industrieanlagen im Iran auch Chemieanlagen, Raffinerien, Kraftwerke und industrielle Produktionsanlagen in China, Großbritannien, Indien, Indonesien, Russland, Südkorea, den USA und auch in Deutschland befallen. Dabei infizierte er sowohl gewöhnliche Windows-PCs, in denen er mangels spezieller Produktionssteuerungssoftware keine Wirkung erzielen konnte, als auch spezielle PCs für Steuerungen. Laut Siemens betrafen ein Drittel der 15 weltweit entdeckten Infektionen deutsche Industrieanlagen. Inzwischen sind weitere Angriffe bekannt geworden. Mitte November fand die IT-Sicherheitsfirma Symantec heraus, dass Stuxnet nur Anlagen angriff, die Frequenzumrichter enthielten, die die Drehzahl von Elektromotoren über die Stromfrequenz steuern, und sofern sie von bestimmten Firmen aus Finnland oder dem Iran hergestellt worden waren. Durch Änderung der Ausgangsfrequenz wird die Arbeitsdrehzahl der Motoren verändert. Der industrielle Prozess wird somit sabotiert.

An der Entwicklung einer solchen Schadsoftware muss ein größeres und gut ausgebildetes Team mit Experten und Ingenieuren für Windows-Programmierung und Automatisierungstechnik beteiligt gewesen sein. Fachleute gehen davon aus, dass aufgrund des erheblichen Programmieraufwands und der hohen Entwicklungskosten die Schadsoftware nicht von einer Privatperson entwi-

28 heise online vom 28. September 2010

ckelt wurde. Es wird nur vermutet, dass sich der Stuxnet-Angriff gezielt gegen iranische Atomanlagen richtete. Jedenfalls war er auf die Schädigung von Industrieanlagen ausgerichtet, die mit ganz bestimmten und spezialisierten Systemen und Programmen ausgestattet waren, die der Steuerung solcher Anlagen dienen und zuvor kaum im Fokus von Softwareangriffen standen.

Im November wurde eine neue Nato-Strategie vorgestellt, die sich mit dem Thema der **Kriegsführung im Cyber-Space** befasst. Der Europarat möchte eine flächendeckende Kontrolle und Überwachung[29]. Hierzu wurde in Vilnius ein Vorschlag zum grenzüberschreitenden Schutz von Internet-Infrastrukturen vorgestellt, der heftig kritisiert wurde, weil hier Voraussetzungen geschaffen würden, die zu einer **flächendeckenden Kontrolle der Internetnutzenden** und deren Verhalten führen. Auch Deutschland hat ein **Computer Emergency Response Team (CERT)** zum Schutz der Militärrechner aufgestellt.

Einerseits fällt es IT-Verantwortlichen immer schwerer, Computer und Daten zu schützen. Die Beschäftigten nutzen zunehmend mobile Geräte wie Smartphones, um von unterwegs auf Unternehmensinformationen zugreifen zu können. Ausländischen Niederlassungen oder Kooperationspartnern muss ebenfalls der Zugriff ermöglicht werden. Ein Unternehmen ohne Internetauftritt wird nicht lange am Markt bestehen. Die Sicherheit muss hier genauso ernst genommen werden wie in der realen Welt. Nicht nur die Technik im Rechenzentrum muss mit einem entsprechenden Zugangsschutz gut geschützt sein, auch die Kommunikationswege müssen gesichert sein. Man spricht nun auch von Sicherheit in der virtuellen Welt. Vernetzte Rechner können zum Risiko werden.

Andererseits sind Unternehmen, sonstige Organisationen sowie Staaten, aber auch Bundesländer wie Berlin immer mehr auf die Nutzung des Internets und damit auf die weltweite Vernetzung der Informationstechnik angewiesen. **„Entnetzung“** ist daher kaum noch möglich. Schließlich ergibt sich daraus eine Angreifbarkeit, die zu empfindlichen finanziellen und politischen Schäden führen kann.

29 F.A.Z. vom 5. Oktober 2010, S. T2

Sicherheitslücken in Computern und Netzwerken können für Unternehmen, Organisationen und Nationen, aber auch für das Land Berlin zu einer Bedrohung werden, weil mit der Störung oder gar der Ausschaltung des Internets die Handlungsfähigkeit der verantwortlichen Stellen ausgeschaltet werden kann. Auch die Verfügbarkeit personenbezogener Daten – ein zentrales Gebot des Datenschutzrechts – wäre dann nicht mehr gegeben.

1.1.2 Georeferenzierte Panoramadienste: Street View war erst der Anfang

Der Start von Google Street View in Deutschland lenkte die Aufmerksamkeit auf eine Entwicklung in der Verarbeitung geografischer Daten, die keineswegs neu ist, aber für die normalen Verbraucherinnen und Verbraucher eher im Verborgenen stattfand: Georeferenzierte Panoramadienste zeigen den Nutzenden fotografische Ansichten von geografischen Orten wie Straßen, Gebäuden und Parks, denen Geokoordinaten zugewiesen sind und die daher online adressgenau aufgerufen werden können.

Landkartendienste wie Google Maps oder stadtplandienst.de arbeiten ebenfalls mit Georeferenzen, die es ermöglichen, mit der Angabe einer Grundstücksadresse auf der Karte punktgenau den Ort anzuzeigen, an dem sich das Grundstück befindet. Beide Dienste bieten ergänzend Luftbilder an, die – insoweit vergleichbar mit Google Earth – jedoch fotografische Draufsichten sind und damit keine Panoramen. Durch die Einbindung von Google Street View in Google Maps in den kleineren Maßstabsbereichen entsteht ein kombinierter georeferenzierter Landkarten- und Panoramadienst.

Der Umgang mit solchen geografischen Daten wurde im vergangenen Jahr unter Datenschutzexperten und in den Medien ausführlich diskutiert. Dabei spielte vor allem die Frage eine Rolle, ob georeferenzierte Panorama- oder Landkartendienste als personenbezogene Dienste angesehen werden müssen und ob daher das Datenschutzrecht überhaupt anzuwenden ist. Die Datenschutzbeauftragten des Bundes und der Länder haben diese Frage von Anfang an bejaht, denn einem Haus kann man seinen Eigentümer oder Mieter zuordnen. Die Gegend, in der ein Haus liegt, kann gut oder schlecht beleumundet sein, für den Eigentümer und die Mieter hat dies Auswirkungen auf den Score-

wert ihrer **Bonität**. Der Zustand des abgebildeten Hauses lässt Rückschlüsse auf die Bereitschaft und finanzielle Fähigkeit zu seiner Erhaltung und damit auf die Bonität des Eigentümers zu.

Google Street View ist bei allem Aufsehen, das die Einführung dieses Dienstes in Deutschland erregte, nicht der einzige Dienst dieser Art. Dass auch andere Kartendienste diese Möglichkeiten anbieten, ist dabei allerdings in den Hintergrund getreten.

Zu den angebotenen Dienstleistungen gehören Panorama- und Landkartenabbildungen, die mit Geodaten verknüpft sind. Die Unterschiede zwischen diesen Diensten sind meist nur sehr gering: Im Allgemeinen zeigen **Panoramadienste** im Internet virtuelle 360-Grad-Ansichten von Stadt und Land. Wer sie nutzt, hat die Möglichkeit, selbsttätig zu navigieren, das Bild zu zoomen oder zu schwenken. Bei dem Datenmaterial handelt es sich um Echtbilder (Standbilder, bisher noch keine Live-Aufnahmen), die die tatsächliche Gebäude- bzw. Landschaftsstruktur zeigen. **Landkartendienste** hingegen verwenden in der Regel schematische, abstrakte Darstellungen, die nur ein symbolisches Abbild der Wirklichkeit wiedergeben. Wie oben erwähnt, bieten einige Landkartendienste neben schematischen Darstellungen auch **Satellitenbilder** an. Reine Geodatendienste zeigen wiederum digital erfasste Bilder von Gebäude- oder Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können. Diese Georeferenzierung kann als Navigations- und Orientierungshilfe genutzt werden.

Im Folgenden sollen exemplarisch einige Panorama-, Landkarten- oder Geodatendienste kurz skizziert werden:

- Die Internetsuchmaschine **Bing** von Microsoft bietet ähnlich wie Google die Möglichkeit, die Suchanfrage in der Kategorie „Landkarten“ anzeigen zu lassen. Dabei können Satellitenbilder in der Draufsicht oder Bilder aus der Vogelperspektive aus allen Himmelsrichtungen betrachtet werden. Ein Heranzoomen ist dabei bedingt möglich.
- Das Projekt **OpenStreetMap** hat das Ziel, freie Geodaten über Straßen, Eisenbahnen, Flüsse, Wälder, Häuser und alles andere, was gemeinhin auf Karten zu sehen ist, zu erfassen. Diese Daten stehen allen Nutzenden lizenzkostenfrei zur Verfügung, um daraus Straßen-, Wander-, Fahrradkarten oder Routenplaner zu erstellen.
- Das Webportal **stadtplandienst.de** wird von dem in Berlin ansässigen Unternehmen Euro-Cities AG angeboten. Das Unternehmen bietet darüber hinaus verschiedene Stadtportale an. Auf stadtplandienst.de kann hausnummerngenau gesucht und das Ergebnis als Karten- oder Satellitenbild betrachtet werden. Es besteht seit 1996 im Internet. Seit 2004 bietet es ein flächendeckendes Kartenwerk im Maßstab 1:10.000 online an.
- **Navteq**, Tochterunternehmen des finnischen Handy-Herstellers Nokia, ist ein US-amerikanischer Anbieter von Geodaten zum Einsatz in Navigationsgeräten. Straßen und andere Objekte werden geometrisch und digital erfasst und an Hersteller von Navigationsgeräten vertrieben. Navteq deckt bisher mit seinen Geodaten im Wesentlichen die westeuropäischen Staaten ab.
- Das niederländisch-belgische Unternehmen **Tele Atlas** ist einer der größten Konkurrenten von Navteq. Tele Atlas ist Hersteller digitaler Karten für Geoinformationssysteme (GIS), standortbezogene Dienste (sog. Location Based Services, LBS) und für Navigationssysteme.
- Beim Panoramadienst **sightwalk.de** wird den Internetnutzenden ein Flanieren aus der Fußgängerperspektive mit 360-Grad-Schwenk durch ausgewählte Straßen einiger deutscher Städte ermöglicht.
- Die Internetseite **berlin-street-view.de** ermöglicht trotz ihres leicht verwirrenden Namens keine freie, flächendeckende Navigation wie Google Street View. Es werden wie bei sightwalk.de ebenfalls ausgewählte Straßen Berliner Kieze im 360-Grad-Schwenk angeboten. Per Mausklick auf eine der angebotenen Straßen wird ein youtube-Video der Straßenszene gezeigt.

Während Landkartendienste wie Google Maps oder stadtplandienst.de trotz der Georeferenz datenschutzrechtlich weitgehend unauffällig blieben, weil keine Panoramabilder gezeigt wurden, war der Start von **Google Street View** im November von großem Medieninteresse begleitet. Seitdem besteht für die Internetnutzenden die Möglichkeit, durch sämtliche Straßen der 20 größten deutschen Städte[30] virtuell zu navigieren.

30 Berlin, Bielefeld, Bochum, Bonn, Bremen, Dortmund, Dresden, Duisburg, Düsseldorf, Essen, Frankfurt am Main, Hamburg, Hannover, Köln, Leipzig, Mannheim, München, Nürnberg, Stuttgart und Wuppertal

Das lückenlose Navigieren durch die Straßen und das Heranzoomen der Bilder erfolgt per Mausklick. Google hat dafür mit Kamerawagen seit 2008[31] 360-Grad-Panoramabilder aus der Perspektive von Passanten angefertigt. Dadurch entsteht der Eindruck, als würden die Nutzenden selbst die Straße entlanggehen und die Gegend um sich herum erkunden.

Der Datenschutz hat bei der Veröffentlichung dieser Bilddaten eine besondere Rolle gespielt, da neben personenbeziehbaren Daten wie Hausfassaden, Autokennzeichen und Grundstücken auch personenbezogene Daten von Passantinnen und Passanten erhoben wurden. Um die Persönlichkeitsrechte der Betroffenen zu wahren, hat Google daher dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit folgende 13 Zusicherungen gegeben:

1. Vor der Veröffentlichung von derartigen Aufnahmen wird eine Technologie zur Verschleierung von Gesichtern eingesetzt.
2. Vor der Veröffentlichung derartiger Aufnahmen wird eine Technologie zur Verschleierung von Kfz- Kennzeichen eingesetzt.
3. Eigentümer und Bewohner können der Darstellung „ihres“ Gebäudes widersprechen, Google wird das Gebäude dementsprechend unkenntlich machen.
4. Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken werden bereits vor der Veröffentlichung von Bildern in einer einfachen Form berücksichtigt mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.
5. Geplante Befahrungen werden mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt gegeben. Die vorhandenen Befahrungspläne werden bis zu zwei Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat außerdem zugesagt, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken.
6. Die Widerspruchsmöglichkeit besteht auch nach der Veröffentlichung.
7. Google benötigt die Rohdaten nach eigenen Angaben zur Weiterentwicklung und Verbesserung der vom Unternehmen entwickelten Technologie zur Unkenntlichmachung von Gesichtern, Kfz-Kennzeichen und Gebäudeansichten. Die Rohdaten werden gelöscht, sobald sie hierfür nicht mehr erforderlich sind.
8. Soweit Personen, Kfz-Kennzeichen und Gebäudeansichten aufgrund eines Widerspruchs zu entfernen sind, müssen auch die entsprechenden Rohdaten gelöscht werden. Ihre Löschung erfolgt bereits vor der Veröffentlichung, wenn der Widerspruch bis zu einem Monat vor Veröffentlichung der Bilder bei Google eingeht. Später oder nach Veröffentlichung eingehende Widersprüche führen zu einer Löschung der Rohdaten binnen zwei Monaten.
9. Es wird ein Verfahrensverzeichnis erstellt.
10. Im Falle von Verknüpfungen des Dienstes durch andere Anbieter behält sich Google in den Nutzungsbedingungen das Recht vor, bei offensichtlicher Verletzung anwendbarer Gesetze dies zu unterbinden.
11. Eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen für Google Street View wird vorgelegt. Insbesondere gehört hierzu auch eine deutliche Beschreibung des Umgangs mit den Widerspruchsdaten von der Entgegennahme des Widerspruchs bis zur endgültigen Löschung.
12. Der Widerspruch kann nach wie vor im Internet unter www.google.de/streetview über den Button „Ein Problem melden“ oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg eingelegt werden.
13. Google bestätigt den Eingang der eingelegten Widersprüche zeitnah.

Bevor Street View in Deutschland startete, konnten Bürgerinnen und Bürger seit April 2009 per Brief oder E-Mail und zusätzlich seit August 2010 auf der Internetseite von Google Maps Deutschland einen Vorabwiderspruch einlegen, damit ihr Haus oder ihre Wohnung bei Street View unkenntlich gemacht wird. Gegen eine Veröffentlichung hatten im Vorfeld rund eine Viertelmillion Bürgerinnen und Bürger aus den 20 Städten[32] Widerspruch eingelegt.

31 Vgl. JB 2008, 8.4.1

32 Vgl. Fn. 29

Da das von Google eingesetzte Verfahren zur Unkenntlichmachung von Abbildungen vor der Veröffentlichung überwiegend automatisiert ablief, war nicht auszuschließen, dass es zu Fehlern kam. Diese führten dazu, dass nicht alle Häuser, Personen oder Kraftfahrzeuge hinreichend unkenntlich gemacht wurden. Auch nach der Veröffentlichung in Street View besteht daher für Bürgerinnen und Bürger die Möglichkeit, die Unkenntlichmachung von Abbildungen zu beantragen.

Sofern sich also Betroffene über einzelne Fehler in der Veröffentlichung bei Street View beschweren oder nachträglich ihr Haus, ihre Wohnung oder ihr Kraftfahrzeug unkenntlich machen lassen wollen, können sie dies auf der entsprechenden Abbildung tun. Auf jeder Abbildung von Street View befindet sich unten links der Button „Ein Problem melden". Wenn etwas zu beanstanden ist, kann diese Anwendung durch Anklicken geöffnet werden. Es erscheint eine Seite, auf der zu meldende Probleme folgenden Rubriken zugeordnet werden können:

- **Bedenken in Bezug auf die Privatsphäre:** Unkenntlichmachung des Gesichts, des eigenen Hauses, des eigenen Autos oder Kfz-Kennzeichens;
- **Unangemessener Inhalt:** z. B. Nacktheit, eigene Person in unangemessener Umgebung;
- **Sonstiges:** falsch positioniertes Bild, falsche Adresse oder falsch ausgerichtete Navigationspfeile, schlechte Bildqualität, mögliche Sicherheitsgefährdung durch Veröffentlichung des Bildes.

Anschließend sollte das Problem in dem dafür vorgesehenen Feld beschrieben werden. Die Angabe einer E-Mail-Adresse ist erforderlich. Es wird empfohlen, dafür eine Adresse zu verwenden, die nicht für private Zwecke genutzt wird. In der Bildvorschau ist der Problempunkt einzugrenzen.

Google hat seine Zusicherungen weitgehend eingehalten. Beim Start des Street View-Dienstes festgestellte Fehler wurden – nach ihrer Meldung – offenbar umgehend beseitigt. Dass Google den Einwänden vieler Menschen in Deutschland – wenn auch erst auf Drängen der zuständigen Aufsichtsbehörde – in dieser Weise entsprochen hat, ist als **Erfolg für den Datenschutz** anzusehen. Nicht nachvollziehbar ist dagegen, weshalb das Unternehmen sich für eine **deutsche „Insellösung"** entschieden und eine Übertragung dieser Praxis

auf andere EU-Mitgliedstaaten oder auf das weltweite Street View-Angebot abgelehnt hat.

Um einen allgemein verbindlichen Rechtsrahmen für georeferenzierte Panoramadienste festzulegen, beschloss der Bundesrat im Juli einstimmig einen **Gesetzentwurf**, der wesentliche Elemente der für Street View vereinbarten Maßnahmen aufgriff[33]. Die Bundesregierung lehnte diesen Gesetzentwurf allerdings umgehend als „Lex Google" ab, der zudem eine zu technikabhängige Regulierung vorsehe. Tatsächlich hat der Bundesrat weder ein verfassungsrechtlich problematisches Einzelfallgesetz vorgeschlagen, noch ging es ihm um die Regulierung einer bestimmten Technik. Die Kritik der Bundesregierung geht deshalb an der Sache vorbei. Das Bundesinnenministerium favorisiert dagegen eine Selbstregulierung durch die Anbieter, gekoppelt mit einer gesetzlich definierten „Roten Linie", die nicht überschritten werden darf[34].

Dementsprechend legte der Branchenverband BITKOM kurz vor Ende des Berichtszeitraums den **Entwurf eines Verhaltenskodexes** für Geodatendienste vor, der zum Ziel hat, einheitliche Grundsätze für alle Anbieter solcher Dienste in Deutschland zu etablieren. Der Entwurf blieb allerdings in mehreren Punkten hinter den von Google für Street View gegebenen Zusicherungen zurück.

Die Datenschutzaufsichtsbehörden werden sich in Gesprächen mit dem BITKOM für entsprechende Verbesserungen einsetzen. Als zuständige Aufsichtsbehörde haben wir den BITKOM außerdem darauf hingewiesen, dass ein Verhaltenskodex nur dann rechtliche Verbindlichkeit erlangt, wenn wir Gelegenheit erhalten, ihn auf die Vereinbarkeit mit dem geltenden Datenschutzrecht zu überprüfen[35]. Diese Prüfung wird sich auch darauf erstrecken, ob die geplanten Verhaltensregeln die Durchführung datenschutzrechtlicher Regelungen fördern, also einen **datenschutzrechtlichen Mehrwert** aufweisen. Dann würde der BITKOM-Verhaltenskodex sich in das vom Bundesgesetzgeber vorgegebene Konzept der „regulierten Selbstregulierung" einfügen.

33 Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, BR-Drs. 259/10 (Beschluss)
34 Vgl. P. König: Rote Linie und Daten-Kodex. In: c't 1/2011, S. 36
35 Vgl. § 38 a BDSG

Grundsätzlich geht es um die Frage, wie frei Bildaufnahmen im öffentlichen Raum künftig sein dürfen. Voraussetzung für eine datenschutzfreundliche Gestaltung aller Panorama-, Landkarten- oder Geodatendienste muss die Berücksichtigung der schutzwürdigen Interessen der Betroffenen sein. Generelle Verhaltensregeln für Geodatendienste sollten sich an den Zusicherungen orientieren, die Google für den deutschen Street View-Dienst gemacht hat.

1.2 Datenverarbeitung in der Berliner Verwaltung

1.2.1 IT-Politik

IT-Planungsrat

Der neue Art. 91 c Grundgesetz (GG) erlaubt Bund und Ländern, bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgaben notwendigen informationstechnischen Systeme zusammenzuarbeiten. Sie können die dafür notwendigen Standards und Sicherheitsanforderungen festlegen. Die Länder dürfen informationstechnische Systeme in gemeinsamen Einrichtungen betreiben. Der Bund errichtet für das Zusammenwirken der Netze des Bundes und der Länder auf Grundlage eines Bundesgesetzes ein Verbindungsnetz.

Zur Koordination dieser Zusammenarbeit nahm der IT-Planungsrat im April seine Arbeit auf. Er hat damit die bisherigen Gremien zur Koordination der Bund-Länder-übergreifenden IT-Projekte (den Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern und den Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung (KoopA ADV)) abgelöst.

Im Mai[36] trat ein Vertrag zur Ausführung von Art. 91 c GG nach Ratifizierung durch alle Bundesländer[37] in Kraft, der die Grundlagen für die Arbeit des Planungsrats beschreibt. Danach hat er folgende Aufgaben:

36 Gesetz zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91 c GG vom 27. Mai 2010, BGBl. I, S. 662

37 Z. B. für Berlin durch Gesetz vom 3. März 2010, GVBl. S. 126

- Koordination der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik;
- Beschluss fachunabhängiger und fachübergreifender IT-Interoperabilitäts- und IT-Sicherheitsstandards;
- Steuerung von Projekten zu Fragen des informations- und kommunikationstechnisch unterstützten Regierens und Verwaltens (E-Government-Projekte), die dem IT-Planungsrat zugewiesen werden;
- Koordination bei der Errichtung des Verbindungsnetzes nach Maßgabe des aufgrund von Art. 91 c Abs. 4 GG ergangenen Bundesgesetzes.

Dem Planungsrat gehören der Beauftragte der Bundesregierung für Informationstechnik sowie je ein für Informationstechnik zuständiger Vertreter jedes Landes an. Beratende Teilnehmer sind drei Vertreter der Gemeinden und Gemeindeverbände sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

In der Geschäftsordnung wurde nach Intervention der Bundesländer geregelt, dass zusätzlich ein Vertreter der Landesdatenschutzbeauftragten an den Sitzungen teilnehmen darf, sofern die Länder betreffende datenschutzrechtliche Belange erörtert werden[38]. Dies entspricht nicht ganz dem Wunsch der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die die **regelmäßige Einbindung der Landesdatenschutzbeauftragten** für geboten hielt[39]. Da jeder Beschluss über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards, gemeinsame E-Government-Projekte und Sicherheitsfragen des Verbindungsnetzes Datenschutzfragen der Länder berühren, dürfte sich faktisch kaum ein Unterschied ergeben.

E-Government in Berlin

In Berlin wurden die Arbeiten an den künftigen E-Government-Strukturen fortgesetzt. Dabei geht es darum, die Online-Anbindung der Bürgerinnen und Bürger an ihre Verwaltung auszubauen und nicht nur einen Bera-

38 Diese Aufgabe nimmt der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern wahr, der auch Vorsitzender des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist.

39 Entschließung vom 8./9. Oktober 2009: Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben, vgl. Dokumentenband 2009, S. 16

tungs- oder Formularservice, sondern nach und nach auch rechtlich verbindliche Verwaltungsdienstleistungen anzubieten, die den Menschen zeitraubende Behördenbesuche ersparen können. **Terminvereinbarungen bei Bürgerämtern, Online-Kraftfahrzeug-Anmeldungen** über Neuwagenhändler, **Online-Beratung von Hörgeschädigten** in der Gebärdensprechstunde über Internet-Videotelefonie, die **Auskunftserlangung über die einheitliche Behörden-Rufnummer D-115** sind bereits heute in Berlin möglich und sollten noch längst nicht das Ende der Möglichkeiten sein. Ein wesentlicher Motor dieser Entwicklung ist auch die technische Umsetzung der europäischen Dienstleistungsrichtlinie, die die verbindliche Auskunftserteilung und den Austausch verbindlicher Dokumente zwischen Dienstleistungsanbietern in Europa und der Institution des Einheitlichen Ansprechpartners über das Internet voraussetzt.[40]

Aber es geht darüber hinaus auch um die technische Unterstützung der aus dem Bürger-Behörden-Kontakt resultierenden Verwaltungsprozesse in den Behörden. Die bislang in papierenen Akten dargestellten Entscheidungsprozesse müssen der elektronischen Akte weichen, die mittels eindeutiger Identifikatoren oder Text-Retrieval-Datenbanken schneller auffindbar ist, die von verschiedenen Stellen aus gleichzeitig gelesen oder gar bearbeitet werden kann, die keinen Archivplatz, sondern quasi unbegrenzt verfügbaren Speicherplatz benötigt.

Das Senatsprogramm **ServiceStadtBerlin** setzt die elektronische Führung verbindlicher Akten voraus. Dies bedeutet, dass die bisher geltenden, häufig strengen Aktenführungsregeln, die die Verbindlichkeit, Beweiskraft und Nachvollziehbarkeit der Aktenführung gewährleisten sollen, auf die elektronische Aktenführung mittels Informationstechnik übertragen werden müssen. Moderne Software für das Dokumentenmanagement und die Vorgangsbearbeitung (DMS/VBS), die diesen Ansprüchen genügen kann, wenn man die vorhandenen Möglichkeiten ausschöpft, existiert längst. Aber mit der Beschaffung der Hard- und Software allein kann das Programm nicht ausgefüllt werden. Komplexer sind die Anpassungen der Behördenstrukturen an diese neuen Arbeitsmethoden und Werkzeuge, die organisatorischen Vorbereitungen, die Abstimmung zwischen unterschiedlichen Interessenvertretungen, die Überwindung von Vorbehalten gegen umfassende technische Neuerungen und die Erziehung der Beschäftigten zu einem neuen Sicherheitsbewusstsein.

40 Vgl. 10.7 sowie JB 2008, 11.5; JB 2009, 10.9

Das Senatsprogramm setzt auch die Änderung von Verwaltungsregelungen voraus. Insbesondere ist die Gemeinsame Geschäftsordnung (GGO) für die Berliner Verwaltung fortzuschreiben, die die neuen Zugangswege der Bürgerinnen und Bürger zu den Behörden und die computergestützte Weiterbearbeitung der Anliegen regeln muss. Wie erfolgt der elektronische Postein- und -ausgang, wie die Mitzeichnungen, wie die revisionssichere Langzeitspeicherung?

Die rechtlichen, organisatorischen, technischen und wirtschaftlichen Rahmenbedingungen des Einsatzes von Dokumentmanagement- und Vorgangsbearbeitungssystemen sind in vier Verwaltungsprojekten untersucht worden. Ein 2. Zwischenbericht wurde dem Senat Anfang 2010 zur Kenntnisnahme vorgelegt[41]. Er konkretisiert den Anpassungsbedarf der Gemeinsamen Geschäftsordnung, die Notwendigkeit eines E-Government-Gesetzes und ergänzender organisatorischer Regelungen für den Übergang von der Papierakte zur elektronischen Akte, den Umgang mit elektronischen Signaturen und E-Mails, der Langzeitspeicherung und Aussonderung von Schriftgut, den Bedarf an Schulungen und den Aufbau eines Landesreferenzmodells für die technischen und organisatorischen Anforderungen an den Einsatz von DMS/VBS.

Für 2011 wurde ein Referentenentwurf für ein **Berliner E-Government-Gesetz** angekündigt. Einen solchen Gesetzentwurf gibt es bisher nur in Schleswig-Holstein[42]. Die Zeitplanung auf Bundesebene sieht vor, dass ein Gesetz bis Ende 2012 verabschiedet wird[43].

1.2.2 IT-Sicherheit

Gegen Jahresende berichteten alle Zeitungen über den erheblichen Anstieg von **Angriffen auf deutsche Behördencomputer,** nach Feststellung des Bundesamtes für Verfassungsschutz zumeist von staatlichen chinesischen Stellen, und von den Plänen der Bundesregierung, ein „Cyber-Abwehr-Zentrum“ einzu-

41 Im Intranet des Landes Berlin: http://www.verwalt-berlin.de/seninn/itk/rahmenbedingungendms_vbs/index.html#sv

42 http://www.landtag.ltsh.de/infothek/wahl16/drucks/2400/drucksache-16-2437.pdf

43 T. Laier: E-Government-Gesetz des Bundes, Vortrag auf der Messe „Moderner Staat 2010“ in Berlin, vgl. http://www.berlin.de/imperia/md/content/verwaltungsmodernisierung/modernerstaat2010/101011_laier_e_government_gesetz.pdf

richten, das diesen Bedrohungen begegnen soll. Diese Angriffe dienen nicht der Sabotage der Behördensysteme, sondern der Ausforschung gespeicherter Geheimnisse. Dennoch werden sie mit dem Thema Cyberkrieg[44] in Verbindung gebracht. Generell stellt sich die Frage der Informationssicherheit deutscher Behördencomputer und damit nicht zuletzt auch der Sicherheit der IT-Systeme und -Anwendungen der Berliner Verwaltung.

Ob die Systeme der Berliner Landesverwaltung das Interesse chinesischer Hacker wecken, ist zweifelhaft. Immerhin ist in den letzten Jahren das Bewusstsein dafür in der Berliner Verwaltung gewachsen, dass die Sicherheit ihrer informationstechnischen Systeme und Verfahren einen höheren Stellenwert genießen muss, wenn man nicht doch einmal als Opfer eigener Fahrlässigkeit oder erfolgreicher Angriffe von außen gezwungen sein will, die Dienstleistungen für Bürgerinnen und Bürger ganz oder teilweise einzustellen.

Die rechtlichen **Regelungen zur Informationssicherheit in Berlin** können zu Recht als **vorbildlich** angesehen werden. Mit ihren Forderungen nach konkreten Maßnahmen lassen sie keinen Raum mehr für Auslegungen, die auf einen Verzicht auf die Umsetzung hinauslaufen. Die selbstverständliche Forderung nach der Angemessenheit der Maßnahmen lässt sich nicht mehr dafür missbrauchen, aus Kostengründen auf das notwendige Sicherheitsniveau zu verzichten, weil angemessene Maßnahmen genau jene sind, die die als nicht tragbar erkannten Risiken auf ein tragbares Maß reduzieren, und nicht jene, die im Verhältnis zu den sonstigen IT-Kosten hinreichend billig sind. Das Niveau der Sicherheitsmaßnahmen hat sich nicht an den Kosten des eingesetzten Verfahrens zu orientieren, sondern am Schutzbedarf der im Verfahren verarbeiteten Daten.

Dies berücksichtigt § 5 BlnDSG. Er verlangt, dass vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung die technischen und organisatorischen Maßnahmen zur Gewährleistung der aufgeführten Schutzziele auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts ermittelt werden müssen. Dabei sollen die Maßnahmen dem angestrebten Schutzzweck angemessen und am jeweiligen Stand der Technik ausgerichtet sein.

44 Vgl. 1.1.1

Die Berliner **IT-Sicherheitsgrundsätze** und die jährlich aktualisierten **IT-Standards** als Verwaltungsvorschriften konkretisieren dies noch. Für alle logisch, organisatorisch oder räumlich zusammengehörigen Bereiche mit einheitlichen Sicherheitsanforderungen, die sog. Sicherheitsdomänen, ist mindestens ein Grundschutz durch Anwendung des IT-Grundschutzkatalogs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu realisieren. Sofern die Schutzbedarfsanalyse (Teil des BSI-Standards 100-2) hohen oder sehr hohen Schutzbedarf ergibt, sind zusätzliche Risikoanalysen (IT-Sicherheitshandbuch des BSI oder BSI-Standard 100-3) erforderlich und darauf aufbauend zusätzliche Sicherheitsmaßnahmen zu ermitteln. Diese Regelung der IT-Sicherheitsgrundsätze folgt den Vorgaben des Verfahrens nach den IT-Grundschutzkatalogen[45].

Als Standard definieren die IT-Sicherheitsgrundsätze Sicherheitskonzepte für die Domänen „Landeseinheitliche IT-Infrastruktur und IT-Dienste“ unter der Vorgabe hohen Schutzbedarfs, „Behörden“ für die verfahrensunabhängige behördliche Infrastruktur sowie „Verfahren“ für die verfahrensspezifischen Sicherheitsanforderungen. Die sog. **verfahrensspezifischen Sicherheitskonzepte** sind diejenigen, die das BlnDSG verlangt. Sie beschreiben die Maßnahmen, die erforderlich sind, um das behördliche Sicherheitskonzept den Besonderheiten des Anwendungsverfahrens anzupassen. Fehlt ein behördliches Sicherheitskonzept, muss das gesetzlich verlangte verfahrensspezifische Konzept um die Maßnahmen ergänzt werden, die auch verfahrensunabhängig für die genutzten Infrastrukturteile in einem behördlichen Sicherheitskonzept enthalten sein müssten. Sonst wäre das Sicherheitskonzept in wesentlichen Bereichen unvollständig.

Die IT-Sicherheitsgrundsätze und die IT-Standards empfehlen zur vereinfachten und vereinheitlichten Umsetzung des Verfahrens nach den IT-Grundschutzkatalogen für behördenübergreifende einheitliche Sicherheitsanforderungen die Anwendung des sog. Modellsicherheitskonzepts. Dieses setzt das Verfahren nach den Grundschutzkatalogen um, berücksichtigt aber vorab alle Regelungen und die Sicherheitsmaßnahmen der zentralen IT-Infrastruktur der Berliner Verwaltung.

45 Eine Ausnahme ist die Option, für Risikoanalysen noch die Methode des IT-Sicherheitshandbuchs von 1992 zu verwenden. Dies ist aus unserer Sicht hinnehmbar.

Damit ist in der Berliner Verwaltung gesetzlich klargestellt, dass verfahrensspezifische Sicherheitskonzepte erstellt werden müssen, und es ist untergesetzlich festgelegt, wie dies zu geschehen hat.

Die IT-Sicherheitsgrundsätze legen auch fest, dass das IT-Kompetenzzentrum bei der Senatsverwaltung für Inneres und Sport einen jährlichen IT-Sicherheitsbericht erstellt. Daraus ergeben sich auf der Basis einer Selbstauskunft der Behörden Jahr für Jahr vergleichbare Zahlen ...

....	2007	2008	2009
über die Anzahl der Selbstauskunft erteilenden Behörden,	71	68	72
die Anzahl der Behörden mit vorliegendem behördlichen Sicherheitskonzept,	47	47	48
wie viele davon von den Behördenleitungen bestätigt wurden,	37	35	36
wie viele gegenwärtig erarbeitet werden,	24	21	23
wie viele Behörden regelmäßige Schulungen vornehmen	27	18	20
bzw. ein IT-Sicherheitsmanagement eingerichtet haben	32	37	43
und wie viele für die IT-Sicherheit keine Ressourcen zur Verfügung stellen.	7	13	15

Die Zahlen zeigen nur wenige Veränderungen, was die Sicherheitskonzepte angeht. Da viele Behörden an solchen arbeiten, sollte man erwarten, dass die Zahlen steigen. Da die Zahl der in Arbeit befindlichen Sicherheitskonzepte ebenfalls relativ konstant bleibt, muss man daraus schließen, dass die Erarbeitung in manchen Behörden als Daueraufgabe angesehen wird, die nicht zu Ende gebracht wird. Unerfreulich ist der nach wie vor geringe Anteil an Behörden, die regelmäßige Schulungen vornehmen, erfreulich dagegen der Anstieg der Zahlen für das IT-Sicherheitsmanagement. Besorgniserregend sind die Selbstauskünfte zur Ressourcenbereitstellung für die IT-Sicherheit, die mittlerweile ein Fünftel der befragten Behörden für entbehrlich hält.

Die Umfrage betrifft die behördlichen Sicherheitskonzepte und gibt keinen Aufschluss darüber, inwieweit die gesetzlich vorgeschriebenen verfahrensspezifischen Sicherheitskonzepte erstellt worden sind. Das Gesetz schreibt solche Konzepte seit 2001 vor, zuvor waren sie schon seit 1999 aufgrund einer Verwaltungsvorschrift zu erstellen. Es muss daher davon ausgegangen werden, dass bei allen IT-Verfahren des Landes seitdem Neukonzeptionen oder wesentliche Änderungen vorgenommen worden sind und deshalb verfahrensspezifische Sicherheitskonzepte vorliegen müssten. Aber selbst bei neuen IT-Verfahren ist es eher die Regel, dass sie ohne Sicherheitskonzepte in Betrieb genommen werden und diese erst irgendwann danach – wenn überhaupt – fertiggestellt werden. Aktuell gilt dies für zwei IT-Verfahren, bei denen man das nicht erwarten sollte, weil sie im Bereich der Eingriffsverwaltung eingesetzt werden:

Seit Januar 2008 betreibt die Senatsverwaltung für Finanzen im Rahmen des Anschlusses an den **EOSS-Verbund** („Evolutionär orientierte Steuersoftware“) ein neues Besteuerungsverfahren, das im Wesentlichen von der bayerischen Steuerverwaltung entwickelt worden ist und für das aufgrund der dortigen Rechtslage kein verfahrensspezifisches Sicherheitskonzept erstellt wurde[46]. Im September 2010 erhielten wir die Mitteilung, dass die Entwicklung eines auf die Berliner Verhältnisse zugeschnittenen Sicherheitskonzepts fortgeschritten sei und dass es uns möglicherweise noch im gleichen Jahr übersandt werden sollte. Dies ist nicht geschehen.

Ende Mai berichtete die Presse, dass ab sofort im **Autobahntunnel Britz** scharf geblitzt wird. Gleichzeitig erhielten wir die „Errichtungsanordnung für das Betreiben einer stationären Geschwindigkeitsüberwachungsanlage Tunnel Ortsteil Britz“. Damit erfuhren wir, dass zur unmittelbaren Auswertung der Schwarzlicht-Überwachungsmaßnahmen im Tunnel Britz ein IT-Verfahren eingesetzt wird, bei dem die Mess- und Bilddaten der Aufnahmekameras auf einen Server in der Tunnelzentrale übertragen, dort auf eine DVD kopiert und damit an die Bußgeldstelle übermittelt werden. Ein verfahrensspezifisches Sicherheitskonzept haben wir in einer ersten Stellungnahme angemahnt. Als Reaktion wurde uns die Fertigstellung einiger Teile mitgeteilt. Nach der Beanstandung des rechtswidrigen Einsatzes des IT-Verfahrens gegenüber der zuständigen Senatorin für Stadtentwicklung teilte diese uns mit, dass sie den Polizei-

46 Vgl. JB 2009, 1.2.2

präsidenten aufgefordert habe, uns die inzwischen fertiggestellten Unterlagen umgehend zuzuleiten. Sie erreichten uns dann am Tag vor Weihnachten. Ihre Prüfung ist noch nicht abgeschlossen.

Festzustellen ist, dass beide genannten hoheitlichen Verfahren rechtswidrig in Betrieb genommen wurden, denn die in § 5 Abs. 3 Satz 1 BlnDSG genannten Voraussetzungen für den rechtmäßigen Einsatz dieser Verfahren waren bei Inbetriebnahme nicht gegeben, für EOSS nach wie vor nicht.

1.2.3 Aktuelle IT-Projekte

Die öffentlichen Stellen des Landes sind verpflichtet, uns über die Einführung neuer Informationsverfahren und wesentliche Änderungen automatisierter Datenverarbeitungen zu informieren[47]. Wann das zu erfolgen hat, ergibt sich aus dem Gesetz nicht. Folgerichtig gibt es öffentliche Stellen, die uns erst unmittelbar vor der Inbetriebnahme unterrichten, sodass eine Beratung zu rechtlichen und technisch-organisatorischen Datenschutzfragen entfallen muss. Jeder dann vorhandene Mangel (z. B. über die Erforderlichkeit hinausgehende Datenerhebungen, fehlendes Sicherheitskonzept) führt zu Mangelfeststellungen oder Beanstandungen, deren nachträgliche Behebung aufwändige Nachbesserungen zur Folge haben. Die Mehrheit der Unterrichtungen erfolgt aber zu einem so frühen Zeitpunkt, dass das vorrangige Ziel der Vorschrift, uns Gelegenheit zur rechtzeitigen Einflussnahme zu geben, erreicht werden kann.

Wir haben erneut diverse neue Verfahren begleitet und begleiten andere nach wie vor. Das im vorigen Abschnitt kritisierte EOSS-Verfahren der Steuerverwaltung wurde erstmals bereits 2007 erörtert[48]. Neu ist das ebenfalls erwähnte IT-Verfahren für die stationäre Geschwindigkeitsüberwachungsanlage Tunnel Ortsteil Britz.

In späteren Abschnitten befassen wir uns ausführlicher mit dem ELENA-Verfahren des Bundes[49], den RFID-gestützten Zutrittskontrollsystemen der Freien

47 § 24 Abs. 3 Satz 3 BlnDSG
48 JB 2007, 1.2.3
49 Vgl. 2.3

Universität Berlin und der Hochschule für Wirtschaft und Recht[50], dem Verfahren WebUntis zur Anwesenheitserfassung in Schulen[51] und der technischen Umsetzung der EU-Dienstleistungsrichtlinie durch die Senatsverwaltung für Wirtschaft, Technologie und Frauen[52].

Die folgenden Projekte sind in unterschiedlichen Stadien der Fertigstellung, aber sämtlich noch nicht ganz abgeschlossen:

E-Government-Verfahren zur Künstlerförderung (eGo-KüF)
Mit dem Projekt soll eine IT-Lösung und durch begleitende organisatorische Maßnahmen die Möglichkeit geschaffen werden, bei der Bearbeitung von Anträgen zur Künstlerförderung den Aufwand zu verringern und die Qualität der Arbeit und den Service für die Antragstellenden zu verbessern. Ihnen werden über ein Internet-Portal Informationen über das Förderverfahren und Antragsformulare zur Verfügung gestellt, die elektronisch ausgefüllt werden können und per E-Mail oder über einen Formularservice eingesandt werden können. Jedoch steht auch der traditionelle Weg über die Übermittlung per Briefpost zur Verfügung. Die weitere Bearbeitung und Verwaltung der Förderanträge erfolgt mit einem Dokumentenmanagement- und Vorgangsbearbeitungssystem (DMS/VBS).

Unsere Beratungsaktivitäten betrafen die rechtliche Grundlage des Verfahrens, die im Gesetz über die Datenverarbeitung im Bereich der Kulturverwaltung enthalten ist, die Aufbewahrungsfristen für die Antrags- und Entscheidungsunterlagen sowie das zunächst fehlende Sicherheitskonzept. Das uns später vorgelegte Sicherheitskonzept war unvollständig und wies erhebliche methodische Schwächen auf. Insbesondere nahm es keinen Bezug auf ein behördliches Sicherheitskonzept, auf dem das verfahrensbezogene Sicherheitskonzept aufbauen muss. Die Erarbeitung eines solchen Konzepts wurde angekündigt.

50 Vgl. 9.1.2
51 Vgl. 9.2.4
52 Vgl. 10.7

Projekt INNOS des Verkehrsverbundes Berlin–Brandenburg

Der Verkehrsverbund Berlin–Brandenburg hat uns zusammen mit der Landesbeauftragten in Brandenburg über das Projekt zur Entwicklung eines „Innovativen interoperablen EFM-Hintergrundsystems – INNOS“[53] informiert, mit dem elektronische Fahrscheine in den Verkehrsbetrieben der Region Berlin–Brandenburg eingeführt werden sollen. Grundlage für das System ist die sog. Kernapplikation des Verbandes Deutscher Verkehrsunternehmen (VDV), die die Kompatibilität und Interoperabilität der elektronischen Fahrscheinsysteme aller deutschen, später vielleicht auch europäischen Verkehrsunternehmen gewährleisten soll, damit mit einem elektronischen Ticket die Benutzung aller Verkehrssysteme möglich ist, ungeachtet der unterschiedlichen Tarifsysteme. Die Kernapplikation ist bereits in der Vergangenheit mit den Datenschutzbeauftragten des Bundes und der Länder und den Datenschutzaufsichtsbehörden abgestimmt worden.

In der ersten Migrationsstufe INNOS-Start sollen nach den Sommerferien 2011 in Berlin, Potsdam, Brandenburg a. d. Havel und Frankfurt/Oder Abonnenten und Jahreskartenbesitzer mit RFID-Chipkarten ausgestattet werden. Beim Einstieg wird die Gültigkeit des elektronischen Tickets mit einem Lesegerät durch Vergleich mit einer Sperrliste geprüft. Gleiches geschieht auch bei einer Fahrkartenkontrolle. Die RFID-Chips enthalten nur jene Daten, die auch bei den heutigen personengebundenen oder nicht personengebundenen Monatskarten eingetragen sind.

Das wichtigste Datenschutzziel bei Projekten zum elektronischen Ticketing ist die Vermeidung von persönlichen Bewegungsprofilen. Dies kann nur erreicht werden, wenn strikt die Prinzipien der Datenvermeidung und Datensparsamkeit, der strengen Zweckbindung und der Trennung von Stamm- und Fahrdaten beachtet werden. Ferner müssen die Datenschutzrechte der Betroffenen beachtet werden. Beim Einsatz von Chipkarten bedeutet dies auch, dass die Fahrgäste Terminals zur Verfügung erhalten, um überprüfen zu können, welche Daten aktuell auf dem RFID-Chip gespeichert werden.[54] Wir werden mit der brandenburgischen Landesbeauftragten das Projekt weiterverfolgen.

53 EFM steht für „Elektronisches Fahrschein-Management“.
54 § 31 c Abs. 2 BlnDSG

Neues Fachverfahren im Landesamt für Gesundheit und Soziales für die Antragsbearbeitung zur Feststellung einer Schwerbehinderung

Das Landesamt für Gesundheit und Soziales (LaGeSo) will 2011 das alte Online-Schwerbehinderten-Antragsverfahren (OSAV) durch ein neues Verfahren ersetzen. Die Prozess- und Arbeitsstruktur soll damit optimiert werden, und alle Internen und Externen (z. B. beauftragte ärztliche Gutachter) sollen künftig online zusammenarbeiten. Auch die Bürgerinnen und Bürger sollen durch die Einbindung eines Online-Formulars einen besseren Service geboten bekommen.

Dies bedeutet, dass Online-Zugriffe von außen auf ein behördliches Verfahren zu realisieren sind, was Sicherheitsfragen aufwirft, die in einem Sicherheitskonzept behandelt werden müssen. Die uns vorgelegte Leistungsbeschreibung für das Verfahren sieht vor, dass die IT-Sicherheitsgrundsätze und die aktuellen IT-Standards Beachtung finden sollen. Das daraus resultierende Sicherheitskonzept wurde für Ende 2010 angekündigt, lag jedoch bei Redaktionsschluss noch nicht vor.

Online-Befragung der Dienstkräfte der Senatsverwaltung für Finanzen im Rahmen des Gesundheitsmanagements

Im Zusammenwirken mit der City BKK[55] und dem Team Gesundheit GmbH, einer Tochtergesellschaft aller BKK-Landesverbände, beabsichtigte die Senatsverwaltung für Finanzen, mit einer freiwilligen Online-Befragung Erkenntnisse über die Arbeitsbedingungen in einigen Abteilungen im eigenen Hause, in der Landeshauptkasse und im Landesamt zur Regelung offener Vermögensfragen/Landesausgleichsamt sowie deren Einfluss auf die Gesundheit und Befindlichkeiten der Dienstkräfte zu erlangen. Das Befragungsergebnis sollte eine detaillierte Auswertung bis hinunter zur Referatsebene und einen davon abhängigen, auf die befragten Organisationseinheiten zugeschnittenen Maßnahmenkatalog enthalten.

Der Fragebogen war schon bei der Abfrage soziodemografischer Daten so differenziert, dass es leicht möglich gewesen wäre, die Personen zu identifizieren, die den Fragebogen ausgefüllt und sich z. B. zu der Arbeitssituation,

55 Betriebskrankenkasse

dem Verhältnis zu Vorgesetzten, dem Betriebsklima und vielen anderen sensitiven Sachverhalten wertend geäußert hätten. Das Verfahren war also als personenbezogen anzusehen. Die Auswertung für die Senatsverwaltung sollte am Ende lediglich aggregierte Daten enthalten, die aus den Fragebögen ermittelt wurden. Wir haben dazu Empfehlungen gegeben, wie bei der Konzeption der Auswertung diesen Risiken entgegengetreten werden kann. Dies bedeutete, dass in den tabellarischen Auswertungen erst Werte ab einer bestimmten Größe auftreten durften, damit der Personenbezug nicht trotz der Aggregierung hergestellt werden konnte. Das Auswertungskonzept wurde in diesem Sinne angepasst, sodass wir keine Vorbehalte mehr hatten.

Digitalisierung der Daten des Katastrophenschutzes (DiDaKat)

Die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz führt ein datenbankgestütztes Katastrophenschutzhandbuch, um in einer konkreten katastrophalen Notfallsituation die erforderlichen Alarme auslösen zu können. Es enthält Rechtsgrundlagen, Kommunikationsverbindungen, Ansprechpartner, Inhalts-, Aufgaben- und Zuständigkeitskataloge, mithin personenbezogene Daten aus den möglicherweise für Notfall- und Krisensituationen relevanten Einrichtungen. Das Katastrophenschutzhandbuch, dessen Rechtsgrundlage in § 4 Abs. 4 Katastrophenschutzgesetz zu finden ist, wird jetzt im Rahmen des Projekts DiDaKat digitalisiert. Dazu ist die Nutzung einer marktgängigen Software vorgesehen, die auf der Grundlage eines Pflichtenheftes ausgewählt wurde.

Es besteht Übereinstimmung, dass auch zu diesem Projekt ein Sicherheitskonzept erarbeitet und umgesetzt werden muss. Dabei geht es weniger um die Vertraulichkeit der personenbezogenen Daten, die einen normalen Schutzbedarf aufweisen, sondern in erster Linie um die Verfügbarkeit der Daten, um sie im unvorhersehbaren Fall des Falles auch nutzen zu können. Kaum weniger wichtig ist die Integrität der Daten, denn fehlerhafte Katastrophenschutzdaten nützen im Ernstfall wenig.

Die Pflege der Daten wird von der Senatsverwaltung und den Bezirken durchgeführt. Es wird darauf ankommen, auf die Abgrenzung und Koordination der verschiedenen speichernden Stellen beim Systembetrieb zu achten. Hier müssen im Rahmen des Betriebskonzepts noch organisatorische Vorgaben erarbeitet werden, die im System umzusetzen sind, um Zuständigkeitsprobleme und

damit Risiken für die Integrität und Verfügbarkeit (auch im Sinne von Vollständigkeit) zu vermeiden.

Wir werden zu den Sitzungen des Abstimmungsgremiums eingeladen und dort die Weiterentwicklung des Projekts begleiten.

Gebärdensprechstunde „Berlin Telefon“ im Versorgungsamt per Videotelefonie

Gehörlose und stark hörgeschädigte Bürgerinnen und Bürger haben die Möglichkeit, Beratungsleistungen des Versorgungsamts im Landesamt für Gesundheit und Soziales (LaGeSo) in Anspruch zu nehmen, die Rücksicht auf ihre Behinderung nehmen. Dafür gibt es einmal monatlich nachmittags die Möglichkeit zu einer persönlichen Sprechstunde mit einer Person, die die Gebärdensprache beherrscht. Andererseits können sich die Hörbehinderten über E-Mail an das Versorgungsamt wenden.

Nunmehr ist eine weitere Möglichkeit geschaffen worden: Davon ausgehend, dass die gehörlosen oder stark hörgeschädigten Bürgerinnen und Bürger im privaten Lebensbereich überdurchschnittlich viel Videotelefonie mit dem Internet-Telefoniesystem Skype nutzen, bietet das Versorgungsamt jetzt den gleichen Kommunikationsweg zum Kontakt mit dem Versorgungsamt, der ebenfalls von einer Person geführt wird, die die Gebärdensprache beherrscht.

Das LaGeSo stellte uns die Frage, in welchem Umfang und in welcher Weise das Unternehmen Skype persönliche Daten der Nutzenden speichert und verarbeitet, weil weder die Allgemeinen Geschäftsbedingungen noch die Datenschutzrichtlinien von Skype darüber hinreichend Auskunft geben.

Wir haben zunächst aus technischer Sicht darauf aufmerksam gemacht, dass der Skype-Dienst zur Erfüllung seines Angebots Sicherheitsmechanismen der Nutzenden umgehen können muss und Mehrwertdienste anbietet, die unbefugt dazu genutzt werden können, unerwünschte Programmcodes auf einen Rechner zu laden und eventuell ausführen zu lassen[56]. Für die Nutzung von Skype wäre es daher erforderlich, dass die Rechner, mit denen Skype verwendet wird,

56 Mehr zu Voice-over-IP und zu Skype vgl. JB 2007, 2.3.1

von anderen Netzen und dem Berliner Landesnetz physisch getrennt werden, um die damit verbundenen Risiken nicht auf diese Netze ausstrahlen zu lassen.

Aus rechtlicher Sicht haben wir festgehalten, dass die Speicherung der Daten bei Skype bei der Anmeldung durch die Nutzerinnen und Nutzer selbst veranlasst wird und daher keinen Bedenken begegnet und dass auch das Gebärdengespräch keine Datenschutzrelevanz hat, da die gesprochenen Inhalte von Skype nach deren Allgemeinen Geschäftsbedingungen und Datenschutzrichtlinien nicht aufgezeichnet werden.

Dennoch haben wir angeregt, den hörbehinderten Menschen Hinweise auf die Praxis der Speicherung von personenbezogenen Daten bei der Nutzung von Skype zu geben. Damit sollen die Nutzenden in die Lage versetzt werden, die Vor- und Nachteile der Skype-Nutzung besser einzuschätzen.

Das LaGeSo sieht für eigene Hinweise jedoch keine Erforderlichkeit und verweist auf den mündigen Menschen, der selbst entscheiden kann, inwieweit er die Allgemeinen Geschäftsbedingungen und Datenschutzrichtlinien von Skype zur Kenntnis nehmen möchte. Diese Aussage erstaunt, weil die Interpretationsprobleme dieser Dokumente beim LaGeSo selbst Ausgangspunkt des Beratungsvorgangs waren. Es wird jedoch daran gedacht, auf den Internetseiten der Gebärdensprechstunde einen gut sichtbaren Hinweis auf die aktuellen Fassungen der Skype-Dokumente aufzunehmen.

Übermittlung von Abrechnungsdaten der Kassenärzte über das KV-SafeNet

Kassenärzte rechnen ihre Leistungen in der Regel mit den Kassenärztlichen Vereinigungen ab. Hierzu übermitteln sie Daten über die behandelten Versicherten, die Diagnosen und die erbrachten Leistungen elektronisch an diese Körperschaften des öffentlichen Rechts. Bisher geschah dies auf Datenträgern, also Disketten oder CDs. Ab dem 1. Januar 2011 verlangt das Gesetz eine leitungsgebundene Übertragung. Hierzu müssen die Praxen an das Internet angeschlossen sein und ein sicherer Übertragungsweg hergestellt werden.

Eine solche Anbindung ist mit Risiken für die Arztpraxen verbunden, denen mit einem sorgfältig geplanten Verfahren begegnet werden muss. In keinem Fall dürfen klar lesbare Patientendaten auf einen Rechner gelangen, von dem aus ein freier Zugriff auf das Internet möglich ist. Setzte sich auf einem solchen Rechner Schadsoftware fest, wären die Patientendaten gefährdet.

Wir haben der Kassenärztlichen Vereinigung Berlin (KVB) einen Anforderungskatalog für die Anbindung der Praxen übergeben. Die sicherste Variante besteht darin, den Rechner, von dem aus die Abrechnungsdaten übertragen werden, vom Praxisnetz zu trennen. Patientendaten dürfen auf ihn nur gelangen, wenn sie bereits verschlüsselt wurden. Eine solche Anordnung ist einfach, kostengünstig und ohne besonderes technisches Fachwissen zu realisieren. Der Rechner kann dann für den allgemeinen Internetzugriff genutzt und muss nicht aufwändig geschützt werden. Wir werden verfolgen, welche Anbindungsvarianten die KVB ihren Mitgliedern anbieten wird, und in den kommenden Jahren stichprobenartig prüfen, ob trotz des Anschlusses der Praxen an das Internet die Sicherheit der Patientendaten gewahrt bleibt.

2. Schwerpunkte

2.1 Gesetz zur Regelung des Beschäftigtendatenschutzes

Die Bundesregierung will nach nahezu dreißigjähriger Diskussion umfassende gesetzliche Regelungen für den Beschäftigtendatenschutz schaffen. Hintergrund ist, dass es zu vielen Fragen des Datenschutzes bei Beschäftigten eine einzelfallbezogene Rechtsprechung der Arbeitsgerichte gibt, die allerdings oft uneinheitlich ist. Obergerichtliche Urteile sind selten. Für zahlreiche in der beruflichen Praxis vorhandene Fragen bestehen keine speziellen gesetzlichen Regelungen. Soweit Regelungen vorhanden sind, finden sie sich in verschiedenen Gesetzen, z. B. im Bundesdatenschutzgesetz, Betriebsverfassungsgesetz, Telekommunikationsgesetz oder Telemediengesetz.

Bereits 1984 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder **Grundsätze für ein Arbeitnehmerdatenschutzgesetz** formuliert[57], die später mehrfach präzisiert wurden[58]. Darin heißt es: *„Wegen der Abhängigkeit des Arbeitnehmers von Arbeitsplatz und Einkommen zur Sicherung seiner Existenz stellt sich für ihn … generell die Pflicht zur Angabe seiner Daten als zwangsweise Erhebung im Sinne der Urteilsgründe (des Volkszählungsurteils) dar. Hieraus ergibt sich für das Beschäftigungsverhältnis die Notwendigkeit einer bereichsspezifischen und präzisen Bestimmung der Verwendungszwecke der erhobenen Daten, des Schutzes vor Zweckentfremdung durch Weitergabe- und Verwertungsverbote sowie der Beschränkung auf das zur Zweckerreichung erforderliche Datenminimum.“*

In der Folgezeit gab es lange keine nennenswerten Bemühungen des Bundesgesetzgebers, ein solches Gesetz auf den Weg zu bringen. Erst als **Konsequenz der Datenskandale** von 2009 (Deutsche Bahn, Lidl, Telekom) und des damit

57 Entschließung vom 27./28. März 1984, vgl. Berliner Datenschutzbeauftragter, Materialien 3 zum Datenschutz: Stellungnahme zum Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 vom 15. Dezember 1983, S. 23, 39 f.

58 Vgl. Entschließung vom 23./24. März 1992, JB 1992, Anlage 2.1; Entschließung vom 27./28. März 2003, Dokumentenband 2003, S. 11, 18 f.; Entschließung vom 8./9. März 2007, Dokumentenband 2007, S. 12

einhergehenden öffentlichen Drucks sah sich der Gesetzgeber zu einer provisorischen „kleinen Lösung“ gezwungen.

Die erste Neuregelung des Beschäftigtendatenschutzes ging auf eine Initiative des Bundesrats im Jahr 2008 zurück. Aus Anlass der genannten Vorfälle zur Beschäftigtenüberwachung bat er die Bundesregierung, durch klare gesetzliche Regelungen die Grenzen der Datenerhebung, -verarbeitung und -nutzung von Beschäftigtendaten zu definieren und Rechtssicherheit für alle Beteiligten zu schaffen. Daraufhin wurde 2009 mit dem neuen § 32 Bundesdatenschutzgesetz (BDSG) ein allgemeiner gesetzlicher Rahmen für den Umgang mit Beschäftigtendaten in Unternehmen geschaffen. Diese Neuregelung sollte ein eigenständiges Beschäftigtendatenschutzgesetz jedoch nicht ersetzen, sondern die bislang von der Rechtsprechung aufgestellten Grundsätze zum Datenschutz in Beschäftigungsverhältnissen zusammenfassen und konkretisieren.

Die Regierungsparteien griffen den Beschäftigtendatenschutz 2009 im Koalitionsvertrag erneut auf. Vorgesehen war, dass wesentliche Fragen des Datenschutzes konkretisiert und der Beschäftigtendatenschutz zukünftig in einem eigenen Abschnitt bzw. Kapitel des Bundesdatenschutzgesetzes ausgestaltet werden sollen. Ergänzend dazu brachte die SPD-Fraktion im Deutschen Bundestag im November 2009 den Entwurf eines Beschäftigtendatenschutzgesetzes ein. Das Bundesministerium des Innern kündigte sodann einen eigenen Gesetzentwurf an.

Ein erster Referentenentwurf des Ministeriums war jedoch in wesentlichen Punkten nicht geeignet, das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle zu erreichen. Zudem blieben eine ganze Reihe von Fragen und Problemen ungeklärt. Die Datenschutzbeauftragten befürchteten, die vorgesehenen Änderungen könnten in zentralen Bereichen des Arbeitslebens sogar eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Sie appellierten an die Bundesregierung, den Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber in einigen Punkten deutlich zugunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Zusammenfassend forderten sie, dass ein Gesetz zur Regelung des Beschäftigtendatenschutzes einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen der Arbeitgebenden und dem verfassungsrechtlich geschützten Persönlichkeitsrecht der

Beschäftigten schaffen müsse. An diesem Anspruch müsse sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdiene.

Am 28. August hat das Bundeskabinett den **Gesetzentwurf zum Beschäftigtendatenschutzrecht** als neuerliches Änderungsgesetz zum BDSG beschlossen[59]. Zuvor war der Entwurf aus dem Bundesministerium des Innern aufgrund der Abstimmung zwischen den Bundesministerien stark verändert und erweitert worden.

Mit dem Gesetz sollen durch umfassende allgemeingültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit erreicht und bestehende Schutzlücken geschlossen werden. Dieser Ansatz ist durchaus zu begrüßen. Er erfordert jedoch klare Begrenzungen durch gesetzliche Verbote der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Besser wäre es daher gewesen, diese notwendigen Regelungen in einem eigenständigen Gesetz zusammenzufassen, statt sie in das BDSG einzufügen.

Auch wenn der Gesetzentwurf zu einigen Verbesserungen beim Beschäftigtendatenschutz führt, ist festzuhalten, dass er auch weiterhin Schwachstellen aufweist, die beseitigt werden müssen, damit die im Entwurf genannten Ziele (Schutz der Beschäftigten vor unrechtmäßiger Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten, Rechtssicherheit für Arbeitgebende und Beschäftigte) erreicht werden können. Wir haben deshalb dem Senat für die Behandlung im Bundesrat **Vorschläge** gemacht, wie der Gesetzentwurf verändert werden sollte:

Große Unsicherheit besteht bei Unternehmen, in welchem Umfang Beschäftigtendaten an eine andere verantwortliche Stelle im Konzern übermittelt werden dürfen. Der Gesetzentwurf enthält hierzu keine Aussage. Die Praxis „behilft" sich bisher häufig damit, Auftragsdatenverarbeitungsverträge abzuschließen, obwohl in Wirklichkeit eine Funktionsübertragung vorliegt. Ein allgemeines Konzernprivileg, das unkontrollierte Datenflüsse innerhalb von Konzernen ermöglichen würde, ist zwar abzulehnen, da dieses zu unbestimmt wäre und ein derartig weitgehendes Privileg nicht erforderlich ist. Es bestehen aber keine Bedenken dagegen, wenn das Beschäftigtendatenschutzgesetz ein

59 BR-Drs. 535/10

eingeschränktes Konzernprivileg für bestimmte klar zu definierende konzernübergreifende Aufgaben innerhalb des Konzerns konstituieren würde. Dies gilt insbesondere, wenn die Datenflüsse verhindern sollen, dass die Konzernmutter für Compliance-Fehler der Tochtergesellschaft selbst haftet. Die schutzwürdigen Belange der Beschäftigten sollten durch größtmögliche Transparenz und eine verschärfte Haftung von Arbeitgebern und Datenempfängern gewährleistet werden.

Verstärkt werden **Whistleblowing-Systeme** in der Wirtschaft angewandt. Eine klare Aussage, ob und wenn ja unter welchen Bedingungen Whistleblowing-Systeme gestattet sind[60], enthält der Gesetzentwurf nicht. Falls der Gesetzgeber Whistleblowing-Systeme als rechtmäßig erachtet, müsste er insbesondere regeln, wie der Schutz der Hinweisgeber, aber auch der zu Unrecht Beschuldigten sichergestellt werden kann. Es müsste verhindert werden, dass sich Beschäftigte über einen langen Zeitraum im „Vorhof des Verdachts" befinden. Auch fehlen Regelungen zum Betrieblichen Eingliederungsmanagement, obwohl dieses sowohl für die Wirtschaft als auch für die Verwaltung verpflichtend und häufig mit der Erhebung und Nutzung sensitiver Gesundheitsdaten verbunden ist.

Der Gesetzentwurf enthält zwar neue Bußgeldtatbestände, darüber hinaus ist es aber notwendig, auch die **rechtswidrige Datennutzung als Ordnungswidrigkeit** auszugestalten. Die Praxis der letzten Jahre hat gezeigt, dass ein ausreichender Beschäftigtendatenschutz nur erreicht werden kann, wenn ausreichende Sanktionsmöglichkeiten bestehen.

Bisher ungeregelt ist die Frage, wie die **Beschäftigtenvertretung** datenschutzrechtlich kontrolliert wird, nachdem das Bundesarbeitsgericht dem betrieblichen Datenschutzbeauftragten des Unternehmens das Recht abgesprochen hat, den Betriebsrat zu kontrollieren[61]. Diese Entscheidung führte zu einem europarechtswidrigen Kontrolldefizit, das der Gesetzgeber durch eine Erweiterung der Kontrollbefugnisse des betrieblichen Datenschutzbeauftragten auf Beschäftigtenvertretungen beenden sollte.

60 Vgl. JB 2008, 8.3.1; JB 2009, 14.1
61 Beschluss vom 11. November 1997 – 1 ABR 21/97, NJW 1998, 2466

Im Gesetz sollte klargestellt werden, dass auch weiterhin **Betriebsvereinbarungen** Rechtsvorschriften nach § 4 Abs. 1 BDSG darstellen. Diese sind insbesondere dann von Bedeutung, wenn das neue Beschäftigtendatenschutzgesetz keine Regelung zum Konzerndatenschutz enthalten sollte. Eine Betriebsvereinbarung sollte es ermöglichen, in gewissem Umfang von Vorschriften des Beschäftigtendatenschutzes abzuweichen, soweit sichergestellt ist, dass – evtl. durch zusätzliche Sicherungen und erhöhte Transparenz – das gesetzliche **Datenschutzniveau nicht abgeschwächt** wird.

Der Gesetzentwurf schränkt die Möglichkeit der **Einwilligung** der Beschäftigten auf die dort ausdrücklich vorgesehene Einwilligung ein.[62] Dies ist zu weitgehend. Es besteht die Gefahr, dass andere durchaus nachvollziehbare, aber im Entwurf nicht genannte Datenverarbeitungen trotz Freiwilligkeit der Einwilligung nicht möglich sind. Zu denken ist etwa an eine konzernweite Skill-Datenbank für Führungskräfte, aber auch an ein Aktienoptionsprogramm, welches bei der US-amerikanischen Muttergesellschaft des Arbeitgebers im Interesse der Beschäftigten durchgeführt wird. Umgekehrt besteht bei einigen im Gesetz geregelten Einwilligungstatbeständen der Betroffenen eher die Gefahr, dass die Einwilligungen nicht freiwillig erfolgen. So wird man kaum davon ausgehen können, dass Beschäftigte im Call-Center freiwillig in die Kontrolle ihrer Arbeitsleistung einwilligen. Anstelle von zweifelhaften Freiwilligkeitsfiktionen ist es sinnvoller, gesetzliche Erlaubnistatbestände und Transparenzregelungen zu schaffen.

Nach dem Gesetzentwurf wird das Recht der Beschäftigten eingeschränkt, sich unmittelbar bei der Kontrollbehörde über den Arbeitgeber zu beschweren.[63] Diese Norm verstößt gegen Art. 28 Abs. 4 Europäische Datenschutzrichtlinie, ist aber unabhängig von diesen rechtlichen Erwägungen auch nicht sachgerecht. Beschäftigte werden in bestimmten Fällen ein Interesse daran haben, sich an die Kontrollbehörde zu wenden, ohne ihre Identität gegenüber dem Arbeitgeber preiszugeben. Darf die **Datenschutzbeschwerde** erst an die Kontrollbehörde gerichtet werden, nachdem der Arbeitgeber ein Abhilfeverlangen abgelehnt hat, weiß dieser, wer sich über ihn beschwert hat. Aus welchem Grund Beschäftigte im Vergleich zu Kundinnen und Kunden eines Unternehmens ein

62 § 32 l Abs. 1
63 § 32 I Abs. 4

eingeschränktes Beschwerderecht haben sollten, ist nicht nachvollziehbar. Da sich im Übrigen jedermann an die Kontrollbehörde wenden kann, führt die Regelung zu dem paradoxen Ergebnis, dass die Beschäftigten zuerst ein Abhilfegesuch an den Arbeitgeber richten müssen, während Dritte die Möglichkeit haben, sich direkt an die Kontrollbehörde zu wenden.

Es besteht auch kein Bedürfnis dafür, von dem Grundsatz der **Direkterhebung bei Betroffenen** in größerem Umfang Ausnahmen zuzulassen, wie dies in § 32 Abs. 6 des Entwurfs geschehen ist. Zu begrüßen wäre es, wenn das Beschäftigtendatenschutzgesetz ein allgemeines **Verbot der Nutzung von Suchmaschinen** zugunsten von Bewerberinnen und Bewerbern enthalten würde. Bei dem jetzigen Entwurf ist zu befürchten, dass sich die Abgrenzung, welche Daten aus dem Internet verwendet werden dürfen und welche nicht, sehr schwierig gestaltet.

Inzwischen wird auch von Seiten der Arbeitgebenden teilweise eingeräumt, dass die Durchführung von **Screening-Verfahren**[64] zu keinen nennenswerten Ergebnissen bei der Aufdeckung von Straftaten geführt hat. Der Gesetzentwurf ermöglicht gleichwohl die Durchführung dieser Verfahren[65]. Die Haupteinschränkung besteht darin, dass der Abgleich (zunächst) in anonymisierter oder pseudonymisierter Form durchzuführen ist. Es fehlen klare materielle Kriterien wie die Prüfung der Verhältnismäßigkeit oder Hinweise auf Unregelmäßigkeiten. Außerdem sollten Arbeitgebende verpflichtet sein, die näheren Umstände, die zu einem Abgleich veranlasst haben, vorab zu dokumentieren.

Es ist erfreulich, dass nach dem Gesetzentwurf die **heimliche Videoüberwachung** von Beschäftigten untersagt werden soll. Zu hoffen bleibt, dass der Gesetzgeber diese Linie trotz des Widerstandes der Wirtschaftsverbände beibehält. Allerdings sollte bei der Videoüberwachung von Beschäftigten nicht zwischen öffentlich und nicht öffentlich zugänglichen Betriebsstätten unterschieden werden. Auch in öffentlich zugänglichen Betriebsstätten wie Kaufhäusern werden Beschäftigte überwacht, die durch § 6b BDSG bisher unzureichend geschützt sind.

64 Vgl. JB 2008, 8.3.1
65 § 32 d Abs. 3

Bei der Frage der **Nutzung von Telekommunikationsdiensten** ist weiterhin ungeklärt, welche rechtlichen Vorgaben Arbeitgebende zu beachten haben, wenn sie den Beschäftigten die private Nutzung von Telekommunikationseinrichtungen gestatten. Auch im Übrigen erscheint die Regelung zur Nutzung von Telekommunikationsdiensten verbesserungswürdig. So wird eine eigenständige Speicherbefugnis zur Leistungs- und Verhaltenskontrolle geschaffen, aber nicht berücksichtigt, dass auch Daten externer Kommunikationspartner betroffen sind. Hier erscheint zumindest prüfenswert, ob bei der Leistungs- und Verhaltenskontrolle nicht – evtl. nur zu Beginn der Kontrolle – mit verkürzten Zielnummern gearbeitet werden kann.

Der Bundesrat hat den Gesetzentwurf begrüßt, gleichzeitig aber Änderungen gefordert. In vielen Punkten hat er sich dabei Empfehlungen der Datenschutzbeauftragten zu eigen gemacht.[66] Die Bundesregierung hat die Forderungen des Bundesrates allerdings weitgehend und ohne überzeugende Begründung abgelehnt[67].

Der Entwurf zum Beschäftigtendatenschutzgesetz muss noch deutlich verbessert werden, um die Beschäftigten wirksam in ihrem informationellen Selbstbestimmungsrecht zu schützen und Rechtssicherheit zu schaffen.

2.2 Neues Datenschutzrecht für die Werbung – kein Lichtblick für die Betroffenen

Mit der „Bundesdatenschutzgesetz-Novelle II“[68] von 2009 hat der Gesetzgeber die Rahmenbedingungen für die Werbung und den Adresshandel geändert. Auslöser für diese Novellierung waren die aufgedeckten Datenskandale, denen ein in großem Stil geführter Handel mit illegal erworbenen personenbezogenen Daten zugrunde lag.

66 BR-Drs. 535/10 (Beschluss) vom 5. November 2010
67 BT-Drs. 17/4230 vom 15. Dezember 2010, S. 87 ff.
68 Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 19. August 2009, BGBl. I, S. 2814

Als Konsequenz aus diesen Skandalen hat der Gesetzgeber den **Grundsatz der Einwilligung** bei der Verwendung von personenbezogenen Daten für Zwecke des Adresshandels und der Werbung festgeschrieben.[69] Gleichzeitig hat er allerdings **diverse Ausnahmetatbestände** vorgesehen. Der Grundsatz erfährt damit erhebliche Einschränkungen. Auch sind die Ausnahmeregelungen stark interpretationsbedürftig. Von der ursprünglichen Intention des Gesetzgebers, die Betroffenen wieder über die Verwendung ihrer personenbezogenen Daten für diese Zwecke selbst entscheiden zu lassen, ist nicht viel übrig geblieben. Auch nach über einem Jahr seit dem Inkrafttreten der Vorschriften herrscht bei vielen Unternehmen Unsicherheit darüber, wie die neuen Rechtsvorschriften zu verstehen sind. Im Folgenden erläutern wir die Neuregelungen und beantworten die ersten Fragen, die uns von verantwortlichen Stellen gestellt wurden.

Soweit Betroffene die Einwilligung in die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zu Werbezwecken erklären, bedarf diese grundsätzlich der Schriftform.[70] Wenn die Einwilligung mit anderen Erklärungen schriftlich erteilt werden soll, z. B. in Allgemeinen Geschäftsbedingungen, ist sie in drucktechnisch deutlicher Form hervorzuheben.[71] Dies kann z.B. durch Fettdruck oder Einrahmungen geschehen.

Soweit die Einwilligung wegen besonderer Umstände nicht der Schriftform bedarf, ist eine schriftliche Bestätigung des Inhalts der Einwilligung notwendig. Diese kann in Textform erfolgen. Es genügt dabei, wenn den Betroffenen der Inhalt ihrer Einwilligung wiedergegeben und deutlich wird, dass und wo die Einwilligung abgegeben wurde, und die Erstellerin bzw. der Ersteller des Bestätigungsschreibens benannt wird. Das Bestätigungsschreiben bedarf keiner eigenhändigen Unterschrift. Eine Bestätigung per (unsicherer) E-Mail ist nur ausreichend, wenn die Betroffenen zu erkennen gegeben haben, dass sie mit dieser Form einverstanden sind.

Der Gesetzgeber hat auch die fortschreitenden technischen Entwicklungen berücksichtigt und Regelungen für Einwilligungen getroffen, die z. B. über das Internet erteilt werden: Bei elektronisch erteilten Einwilligungen darf von der

69 § 28 Abs. 3 Satz 1 BDSG
70 § 4a Abs. 1 Satz 3 BDSG
71 § 28 Abs. 3a Satz 2 BDSG

Schriftform ohne Bestätigungsschreiben abgewichen werden. Allerdings muss das Unternehmen hier technisch sicherstellen, dass die Einwilligung protokolliert wird und die Betroffenen jederzeit den Inhalt der Einwilligung abrufen können. Zudem muss für die Betroffenen die Möglichkeit bestehen, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.[72]

Vom Grundsatz der erforderlichen Einwilligung bei der Verwendung von personenbezogenen Daten für Zwecke der Werbung hat der Gesetzgeber folgende **Ausnahmen** vorgesehen:

- Eigenwerbung,
- berufliche Werbung,
- Spendenwerbung,
- transparente Werbung und
- transparente Nutzung.

Bei diesen Ausnahmen ist stets zusätzlich zu prüfen, ob dennoch schutzwürdige Interessen der Betroffenen der Verarbeitung oder Nutzung entgegenstehen[73]. Selbst wenn das nicht der Fall ist, haben die Betroffenen stets ein **Widerspruchsrecht**[74].

Ausnahme „Eigenwerbung“ (§ 28 Abs. 3 Satz 2 Nr. 1 BDSG)

Unternehmen dürfen personenbezogene Daten für eigene Werbeangebote auch verarbeiten und nutzen, wenn die Betroffenen nicht eingewilligt haben. Voraussetzung ist, dass sog. Listendaten verwendet werden. Listendaten sind die Zugehörigkeit von Betroffenen zu einer Personengruppe, die Berufs-, Branchen- oder Geschäftsbezeichnung, der Name, Titel, akademische Grade, die Anschrift und das Geburtsjahr. Ferner müssen die Unternehmen diese Daten bei den Betroffenen entweder im Rahmen oder im Vorfeld eines Schuldverhältnisses (z. B. Kaufvertrag oder Vertragsverhandlungen)[75] oder diese Daten

72 § 28 Abs. 3a Satz 1 BDSG
73 § 28 Abs. 3 Satz 6 BDSG
74 § 28 Abs. 4 Satz 1 BDSG
75 § 28 Abs. 1 Satz 1 Nr. 1 BDSG

aus allgemein zugänglichen Verzeichnissen wie Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse erhoben haben. Einzeln aufzufindende Angaben aus dem Internet dürfen daher nicht verwendet werden. Es ist aber zulässig, Daten aus Gewinnspielen für Werbezwecke zu verwenden. Wichtig ist, dass die Unternehmen nicht nur bei der Werbeansprache, sondern bereits bei der Erhebung der Daten im Rahmen oder im Vorfeld eines Schuldverhältnisses auf die Möglichkeit hinweisen, dass die Betroffenen der Verarbeitung oder Nutzung der Daten für Werbezwecke widersprechen können.[76] Erfolgt dieser Hinweis nicht, ist bereits ein Bußgeldtatbestand erfüllt.[77] Wir haben in solchen Fällen mehrfach Bußgelder verhängt.

Um den Unternehmen eine gezielte Ansprache zu ermöglichen, dürfen sie weitere Daten zu den Listendaten hinzuspeichern[78]. Das Hinzuspeichern findet allerdings seine Grenze dort, wo Datenprofile gebildet werden und daher die schutzwürdigen Interessen der Betroffenen entgegenstehen. Ferner dürfen Daten nur hinzugespeichert werden, wenn eine eigene Verarbeitung oder Nutzung von Daten zu Werbezwecken erfolgt. Eine Datenübermittlung dieser angereicherten Daten ist nicht erlaubt. Das Hinzuspeichern von Daten ist nur für eigene Angebote der jeweils verantwortlichen Stelle gestattet.

Ausnahme „berufliche Werbung“ (§ 28 Abs. 3 Satz 2 Nr. 2 BDSG)

Listendaten dürfen auch für die Werbung im Hinblick auf die berufliche Tätigkeit von Betroffenen verarbeitet und genutzt werden. Unternehmen dürfen Werbung daher auch ohne Einwilligung an die Geschäftsadresse von Betroffenen versenden. Die Werbung muss allerdings einen Bezug zur beruflichen Tätigkeit aufweisen. Von dieser Ausnahme sind damit überwiegend Freiberufler betroffen. Es ist aber auch möglich, personifizierte Werbung an Beschäftigte eines Unternehmens unter der Geschäftsadresse des Unternehmens zu versenden. So darf ein Fortbildungsinstitut einem Sachbearbeiter der Personalabteilung ein an ihn adressiertes Werbeschreiben unter der Geschäftsadresse des Unternehmens zu aktuellen Fortbildungen im Personalbereich übersenden. Auch hier ist jedoch zu beachten, dass das Werbeschreiben einen Hinweis

76 § 28 Abs. 4 Satz 2 BDSG
77 § 43 Abs. 1 Nr. 3 BDSG
78 § 28 Abs. 3 Satz 3 BDSG

enthalten muss, dass die Betroffenen der Zusendung von Werbung widersprechen können.[79]

Ausnahme „Spendenwerbung“ (§ 28 Abs. 3 Satz 2 Nr. 3 BDSG)

Listendaten dürfen auch für steuerbegünstigte Spendenwerbung verwendet und genutzt werden. Auch bei dieser Werbeform ist im Werbeschreiben darauf hinzuweisen, dass Betroffene der Verarbeitung oder Nutzung ihrer Daten für Werbezwecke widersprechen können.

Ausnahme „transparente Werbung“ (§ 28 Abs. 3 Satz 4 BDSG)

Eine Übermittlung eigener Kundendaten an andere Unternehmen ist auch nach der Novellierung des Bundesdatenschutzgesetzes möglich. Listendaten dürfen für Werbezwecke an Dritte übermittelt werden. Voraussetzung für eine solche rechtmäßige Datenübermittlung ist, dass Übermittelnde und Empfangende die Tatsache der Übermittlung sowie die Herkunft der Daten und den Empfänger für zwei Jahre speichern.[80] Generell ist zu speichern, welche Stelle die Daten erstmalig erhoben hat, denn dies muss im Werbeschreiben ebenfalls den Betroffenen eindeutig mitgeteilt werden. Die Betroffenen sollen erkennen können, wer ihre Daten weitergegeben hat. Der Gesetzgeber erhofft sich von dieser Transparenzanforderung einen „dämpfenden Effekt“[81] für die erstmalig erhebende Stelle, personenbezogene Daten für Zwecke der Werbung zu verarbeiten. Unter Beachtung dieser Anforderungen dürfen auch Adresshändlern Daten übermittelt werden. Diese dürfen ihrerseits die an sie übermittelten Daten unter Beachtung der Transparenzanforderungen weiterübermitteln.

Ausnahme „transparente Nutzung“ (§ 28 Abs. 3 Satz 5 BDSG)

Listendaten können auch für fremde Werbeangebote genutzt werden. Eine Datenübermittlung und damit Bekanntgabe von personenbezogenen Daten zwischen den Unternehmen findet in diesen Fällen nicht statt. Unternehmen dürfen daher ihrer eigenen Werbung fremde Werbung beifügen („Beipackwerbung“). Fremdwerbung darf aber auch z. B. beim Rechnungsversand beigepackt werden. Erlaubt ist auch eine empfehlende Werbung, bei der ein Unternehmen seinen Kunden im eigenen Namen, aber fremden Interesse Produkte von Kooperationspartnern empfiehlt („Empfehlungswerbung“). Voraussetzung ist allerdings, dass aus dem Werbeschreiben eindeutig hervorgeht, wer die für die Nutzung der Daten verantwortliche Stelle ist. Es muss deutlich werden, wer die Kundendaten für die Werbung Dritter einsetzt. Weiterhin bleibt es möglich, Listendaten bei anderen Unternehmen anzumieten. Diese durchforsten dann ihre Datenbestände nach Konsumenten und versenden die Werbung. Eine Datenübermittlung findet bei diesem Verfahren ebenfalls nicht statt. Auch hier muss bei den Werbeschreiben an die Betroffenen ein entsprechender Hinweis auf das Unternehmen erfolgen, das als verantwortliche Stelle seine Daten weitervermietet hat.

Ebenfalls ist bei der transparenten Nutzung eine Abwägung mit den schutzwürdigen Interessen der Betroffenen geboten.[82] Soweit diese entgegenstehen, darf eine solche Nutzung zu Werbezwecken nicht stattfinden. Zwar wird eine solche Abwägung für die transparente Nutzung nicht ausdrücklich im Gesetzeswortlaut genannt. Hierbei handelt es sich jedoch um ein redaktionelles Versehen, da bei den Beratungen zur Novellierung des Bundesdatenschutzgesetzes im Deutschen Bundestag die eingefügten Änderungen nicht vollständig überarbeitet und angepasst wurden.

Werbung durch politische Parteien

Bei politischen Parteien besteht Unsicherheit, ob die Regelungen für Werbeschreiben auch bei politischer Werbung (etwa im Wahlkampf) gelten. Teilweise wird differenziert zwischen politischer Werbung und Information über Sachthemen. Von der Klärung dieser Frage ist insbesondere abhängig, ob Werbeschreiben einen Hinweis auf den Werbewiderspruch enthalten müssen[83] und ob bei Fremdwerbung ein Hinweis auf die verantwortliche Stelle gegeben werden muss.[84]

79 § 28 Abs. 4 Satz 2 BDSG
80 § 34 Abs. 1a BDSG
81 BT-Drs. 16/13657, S. 19
82 § 28 Abs. 3 Satz 6 BDSG
83 § 28 Abs. 4 Satz 2 BDSG
84 § 28 Abs. 3 Satz 5 BDSG

Vom Begriff „Werbung“ werden alle Formen der Ansprache sowie die Darstellung eigener ideeller oder politischer Ziele oder Aufrufe zur Unterstützung erfasst. Eine Privilegierung der politischen Parteien gegenüber anderen werbenden verantwortlichen Stellen sieht das Gesetz nicht vor. Dies ergibt sich auch aus dem Umkehrschluss zu § 28 Abs. 3 Satz 2 Nr. 3 BDSG, nach dem das Gesetz Privilegierungen nur bei Werbung für Spenden vorsieht. Aber selbst Spendenunternehmen werden von der Pflicht, auf den Werbewiderspruch hinzuweisen, nicht befreit. Teilweise wird die Auffassung vertreten, dass die Regeln über Werbung nicht gelten, wenn politische Parteien sich zu Sachthemen äußern und hierdurch das ihnen zustehende Recht ausüben, an der politischen Willensbildung mitzuwirken.[85] Diese Rechtsauffassung ist allerdings unzutreffend, da die Einhaltung der werberechtlichen Regelungen die Parteien nicht an ihrem verfassungsrechtlichen Recht auf Mitwirkung an der politischen Willensbildung hindert.

Die Verwendung von personenbezogenen Daten für Werbezwecke wird auch durch das 2009 geänderte Bundesdatenschutzgesetz zu stark zu Lasten der Betroffenen privilegiert. Von der ursprünglichen Absicht der Bundesregierung, der informationellen Selbstbestimmung durch ein zwingendes Erfordernis der Einwilligung Geltung zu verschaffen, ist nicht viel übrig geblieben. Die jetzt geltende Regelung mit ihren zahlreichen Ausnahmen wirft erhebliche Auslegungsprobleme auf.

2.3 Der Elektronische Entgeltnachweis (ELENA) – ein unsicherer Daten-Moloch

Seit Anfang des Jahres sind Unternehmen und öffentliche Dienstherren gesetzlich verpflichtet, Daten über das gezahlte Entgelt und weitere Angaben über ihre Beschäftigten an die Zentrale Speicherstelle des ELENA-Verfahrens zu übermitteln.

85 Art. 21 Abs. 1 Satz 1 GG

Der Elektronische Entgeltnachweis soll dazu dienen, die bisherige papiergebundene Übermittlung von Bescheinigungen der Unternehmen an die Bundesagentur für Arbeit, die Wohn- und die Elterngeldstellen durch elektronische Meldungen abzulösen. Es werden jedoch nicht nur die Daten derjenigen gesammelt und übertragen, die Anträge auf Sozialleistungen stellen. Stattdessen werden die Daten aller Beschäftigten auf Vorrat gespeichert (von denen nur ein Bruchteil jemals einen Entgeltnachweis benötigen wird) und nur im Bedarfsfalle abgerufen.

Wir bezweifeln, dass diese immense **Vorratsdatenspeicherung** verfassungsgemäß ist. Dem Bundesverfassungsgericht liegt eine große Zahl von Verfassungsbeschwerden gegen das ELENA-Verfahrensgesetz vor. Legt man die Kriterien zugrunde, die das Gericht in seinem Urteil zur Vorratsdatenspeicherung[86] formuliert hat, spricht vieles dafür, dass das Gesetz für verfassungswidrig erklärt wird. Denn es ist schon fraglich, ob das ELENA-Verfahren, das ausschließlich der **Verwaltungsvereinfachung** für die Unternehmen dienen soll, ein legitimer Gemeinwohlzweck ist, der den Aufbau einer zentralen Datenbank mit den Daten aller Beschäftigten in Deutschland rechtfertigen kann. Jedenfalls führt eine solche Datenbank zu **unverhältnismäßigen Eingriffen in das Grundrecht auf Datenschutz** vor allem derjenigen Menschen, die zu keiner Zeit eine Entgeltbescheinigung benötigen werden (z.B. Beamtinnen und Beamte). Es sind zudem andere dezentrale Modelle der anlassbezogenen Erteilung von elektronischen Entgeltbescheinigungen denkbar, die eine solche bundesweite Datensammlung überflüssig machen.

Trotz unserer Zweifel an der Verfassungsmäßigkeit war es erforderlich, die Vorgehensweise für den Abruf der Daten durch Stellen, welche in die Zuständigkeit des Landes fallen, zu begleiten und auf ein gesetzeskonformes Vorgehen und ein möglichst hohes Datenschutzniveau hinzuwirken. Diese Aufgabe haben wir in beratender Rolle in der Arbeitsgruppe zu Informationssicherheit und Datenschutz des Bund-Länder-Arbeitskreises „ELENA-Verfahrensgrundsätze“[87] übernommen.

86 NJW 2010, 833 ff.; vgl. dazu auch 13.1
87 Vgl. § 28b Abs. 2 und 6 SGB IV

Wir mussten feststellen, dass die vorgesehenen komplexen Verfahren in wesentlichen Punkten von den gesetzlichen Vorgaben abweichen und die Daten der von der Zentralen Speicherstelle erfassten Betroffenen erheblichen Risiken aussetzen.

Im Vorfeld der Ausarbeitung des ELENA-Verfahrensgesetzes hatten die Landesdatenschutzbeauftragten gefordert, dass die von den Unternehmen an die Zentrale Speicherstelle gemeldeten Daten so verschlüsselt (und dann erst gespeichert) werden, dass nur die oder der Betroffene sie mit einer speziellen **Chipkarte** (damals sog. Jobcard) entschlüsseln kann. Die Kosten der Ausgabe dieser Karte wollten jedoch weder die öffentliche Hand noch die Wirtschaft übernehmen.

Daher werden die Meldedaten nunmehr nicht unter den Klarnamen der Betroffenen gespeichert und in einem zweistufigen Verfahren derart verschlüsselt, dass nur der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) mithilfe einer besonders geschützten Anlage die Entschlüsselung vornehmen kann[88]. Damit ist es allen, die unberechtigt direkt auf die Datenbank der Zentralen Speicherstelle zugreifen, zunächst unmöglich, die Daten zu interpretieren und einzelnen Personen zuzuordnen.

Um zu einer Person die vorliegenden Meldungen zu finden, nutzt die Speicherstelle die im Abrufantrag enthaltenen Daten und kommuniziert mit einer zweiten Stelle, bei der sich die Betroffenen, die einen Nachweis benötigen, zu registrieren haben (sog. Registratur Fachverfahren[89]). Die Daten derart registrierter Betroffener lassen sich allerdings auch ohne Angaben in einem Abrufantrag auffinden. Für diese Personen ist eine Kennnummer, unter der die Daten abgelegt werden, regelmäßig in einem öffentlichen Verzeichnis enthalten, das zur Überprüfung der vorgeschriebenen elektronischen Signatur geführt wird[90].

Zur Erfüllung ihrer Aufgaben kann die Zentrale Speicherstelle selbst jederzeit die Entschlüsselung eines Datensatzes beauftragen. Solche Aufträge, von denen jeden Tag Hunderttausende bei dem BfDI eingehen werden, hat dieser ungeprüft auszuführen. Es ist allein Aufgabe der Zentralen Speicherstelle, die Voraussetzungen zu überprüfen, unter denen eine Entschlüsselung und Übermittlung an eine abrufende Stelle (z.B. eine Wohngeldstelle) erfolgen darf[91]. Die Beschäftigten der Speicherstelle müssen deshalb absolut vertrauenswürdig arbeiten.

Zwei Voraussetzungen sind wesentlich: Die Betroffenen müssen ihr Einverständnis erklärt und eine Behördenmitarbeiterin oder ein Behördenmitarbeiter muss den Abruf autorisiert haben. Die Betroffenen müssen ihr Einverständnis nicht unbedingt selbst erklären. Sie können gesetzlich vertreten werden oder sie können für diesen Zweck Dritte beauftragen. Eine solche Beauftragung muss in der Anmeldestelle, welche in der Regel mit der abrufenden Stelle übereinstimmt, wiederum sorgfältig geprüft werden. Eine fehlerhaft anerkannte oder missbräuchlich fingierte Bevollmächtigung kann dazu führen, dass die Daten ohne Kenntnis und Willen der Betroffenen abgerufen, verarbeitet und Dritten offengelegt werden.

Damit liegt die Sicherheit des ELENA-Datenbestandes in den Händen der bei den anmeldenden und abrufenden Stellen tätigen Personen. Besonders gefährdet sind solche (kleinen) Stellen, in denen in unmittelbarer Nähe oder gar von den gleichen Personen die Anmeldung einer oder eines Teilnehmenden bzw. die Bestätigung von Vollmachten vorgenommen und die Abrufe in Auftrag gegeben werden. Arbeitet auch nur eine Person in einer dieser Stellen unzuverlässig oder handelt missbräuchlich, so stehen ihr die Daten aller Beschäftigten in Deutschland offen.

Daher ist es wichtig, wenigstens im Nachhinein feststellen zu können, wer welche Aktion im Rahmen des ELENA-Verfahrens vorgenommen hat. Dazu dienen technische Mittel, die der Gesetzgeber wenigstens für den Abruf der Daten, nicht jedoch für die Anmeldung der Teilnehmenden, Vertretenden und Bevollmächtigten selbst vorgegeben hat. Um Kosten zu sparen, lehnen die Verfahrensträger jedoch den Einsatz derartiger Mittel, sog. qualifizierter Signaturkarten und der zugehörigen Infrastruktur, für ihre Verwaltung ab.

88 § 99 Abs. 3 SGB IV
89 § 100 SGB IV
90 § 99 Abs. 6 SGB IV und § 5 Abs. 1 Signaturgesetz
91 § 99 Abs. 3 SGB IV

Darüber hinaus soll in einer Verfahrensvariante den abrufenden Stellen die Möglichkeit eröffnet werden, die technische Überprüfung der Identität der abrufenden Bediensteten, die der Gesetzgeber der vertrauenswürdigen Zentralen Speicherstelle zugewiesen hat, selbst zu übernehmen. Dieses Vorgehen lehnen wir ab, zumindest solange die entstehenden Risiken nicht auf gesetzlicher Grundlage anders kompensiert werden.

Besonders problematisch ist, dass die Zentrale Speicherstelle ihrer gesetzlichen Pflicht, die abrufenden Behörden bei ihrer Zulassung zur Teilnahme an dem Verfahren auf die Gewährleistung von Datenschutz und -sicherheit zu überprüfen, nur höchst rudimentär nachkommen wird, indem sie sich die Vornahme bestimmter Maßnahmen bestätigen lässt. Dies ist selbst in dieser Form bereits ein Erfolg unserer Überzeugungsarbeit: Ursprünglich sollte die bloße Aussage der Leitung der abrufenden Behörde genügen, der Datenschutz werde eingehalten. Jetzt erklärten sich die Verfahrensträger auf Veranlassung der an der Arbeitsgemeinschaft beteiligten Datenschutzbeauftragten bereit, einen Maßnahmenkatalog zusammenzustellen und in einer Handreichung den abrufenden Behörden zur Verfügung zu stellen, dessen Umsetzung einen Grundschutz des Datenabrufs bewirken wird.

Wenn ein Zugriff auf die Daten der Bürgerinnen und Bürger zwar rechtlich ihre Mitwirkung voraussetzt, das Vorliegen dieser Mitwirkung jedoch technisch nicht durchweg überprüfbar bleibt, sondern zu missbräuchlichen Zwecken im Einzelfall fingiert werden kann, und wenn die technische Nachverfolgbarkeit von unzulässigen Datenabrufen in Frage steht, können die Betroffenen wenigstens selbst nachprüfen, ob und welche Daten zu ihrer Person gespeichert und wem sie übermittelt wurden?

In der Tat haben die Betroffenen hierzu ein gesetzlich verbrieftes Auskunftsrecht. Entgegen unserer mehrfachen Mahnung wird es erst 18 Monate nach Aufnahme der Datenspeicherungen (voraussichtlich Mitte 2012) möglich sein, dieses Auskunftsrecht wahrzunehmen. Auch dann werden **mit einem Auskunftsersuchen außerordentliche Kosten verbunden** sein. Auskunftsuchende müssen sich im Einklang mit dem allgemeinen Abrufprozedere eine Chipkarte für derzeit 50 Euro jährlich beschaffen und damit ihr Auskunftsersuchen elektronisch unterzeichnen. Diese Kosten werden ihnen jedoch nicht ersetzt. Das Auskunftsrecht wird damit de facto ausgehebelt.

Das ELENA-Verfahren ist mit einer immensen Vorratsdatenspeicherung verbunden, die einzig dem Zweck der Verfahrensvereinfachung dient. Es führt deshalb zu unverhältnismäßigen Eingriffen in das Grundrecht auf Datenschutz aller abhängig Beschäftigten, Beamtinnen und Beamten, Richterinnen und Richtern, Soldatinnen und Soldaten. Die gesetzlichen Regelungen gewährleisten den Schutz des massiven ELENA-Datenbestandes unzureichend. Sie werden dazu nicht vollständig umgesetzt. Wir halten die Risiken, die mit dem ELENA-Verfahren entstehen, nicht für tragbar.

2.4 Der neue Personalausweis

Seit dem 1. November gibt es den neuen elektronischen Personalausweis für alle Bundesbürgerinnen und -bürger. Er soll sie wie bisher an der Grenze und im Inland gegenüber staatlichen Stellen identifizieren. Er soll darüber hinaus auch das Internet sicherer machen und rechtssichere elektronische Anwendungen ermöglichen. Aber der neue Personalausweis kann weiterhin wie der bekannte Personalausweis verwendet werden, nur mit dem Unterschied, dass die elektronisch zu lesenden Daten in einem RFID-Chip[92] gespeichert und nicht wie bisher als elektronisch lesbare OCR-Schrift auf dem Ausweis aufgedruckt sind. Alle weiteren Funktionen sind freiwillig.

Der neue Personalausweis hat Kreditkartenformat. Der darin integrierte Chip kann kontaktlos ausgelesen werden. Auf dem Ausweis sind alle Daten wie bisher aufgedruckt. Neu ist, dass nicht nur diese Daten auf einem elektronischen Chip abgespeichert sind und von einem Lesegerät ausgelesen werden können, sondern dass dieser Chip auch weitere Daten für zusätzliche Anwendungen speichern kann.

Zusätzlich zu den bisherigen Daten können die Bürgerinnen und Bürger freiwillig auch Fingerabdrücke auf dem Chip abspeichern lassen. Diese werden bei der ausstellenden Behörde nur so lange gespeichert, bis die oder der Berechtigte den neuen Ausweis abgeholt hat. Eine dauerhafte zentrale Speicherung erfolgt nicht. Wer den neuen Personalausweis beantragt, sollte trotzdem gut

92 RFID-Chip: Radio Frequency IDentification

überlegen, ob er diese sensiblen Daten auf dem Chip des Personalausweises speichern lassen möchte. Bisher ist nicht zu erkennen, welche Vorteile Betroffene von der Speicherung ihrer Fingerabdrücke haben könnten. Vielmehr werden diese biometrischen Merkmale dadurch einem zusätzlichen Missbrauchsrisiko ausgesetzt.

Neben der Funktion der Identifikation gegenüber Behörden bietet der neue Ausweis zwei neue elektronische Funktionen:

- Elektronische Identitätsfunktion im Internet (eID)
- Qualifizierte elektronische Signatur (QES)

Der neue Personalausweis soll im Internet den gleichen Identitätsnachweis liefern, wie es die Funktion als Sichtdokument im normalen Leben schon bietet. Die Ausweisinhaberinnen und -inhaber sollen die Möglichkeit bekommen, sich online gegenüber Dritten eindeutig und authentisch auszuweisen (**eID-Funktion**). Dies gilt sowohl für E-Government-Anwendungen im öffentlichen Bereich als auch für private Anbieter im Internet. Wer diese Funktion nutzen will, braucht dafür eine spezielle Anwendungssoftware für den PC, die sog. AusweisApp. Dies ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Software, die die Kommunikation mit den Internet-Anbietern übernimmt und dafür sorgen soll, dass persönliche Daten sicher über das Internet übertragen werden können. Direkt nach der Einführung wurde hier ein schwerwiegender Sicherheitsmangel bekannt, denn es war möglich, über die Aktualisierungsfunktion der Software schädliche Programme auf den heimischen PC der Ausweisinhaberinnen und -inhaber einzuschleusen. Dieser Sicherheitsmangel ist mittlerweile behoben.

Wer die eID-Funktion nutzen will, braucht zusätzlich ein spezielles Lesegerät, das die Daten aus dem Chip des neuen Personalausweises ausliest. Hier gibt es drei verschiedene Arten von Geräten, die sich in der Sicherheit deutlich unterscheiden. Die einfache und kostengünstigste Variante ist ein Basislesegerät ohne eigene Tastatur für die Eingabe der sechsstelligen Geheimzahl (PIN), die die Berechtigten beim Abholen des neuen Personalausweises festlegen müssen. Die beiden anderen Varianten verfügen über ein eigenes Eingabefeld für die Geheimzahl. Bei der Nutzung des einfachen Basislesegerätes muss die PIN über die PC-Tastatur eingegeben werden. Hat jemand Schadsoftware auf dem PC,

die die Tastatureingaben mitschneidet (sog. Keylogger), kann es zum „Abhören“ der Geheimzahl kommen. Kennt ein Angreifer die Geheimzahl und hat es geschafft, weitere Schadsoftware auf dem PC zu installieren, könnte er im Namen des jeweiligen Personalausweisinhabers Geschäfte im Internet tätigen. Wir empfehlen daher dringend die Nutzung eines Komfortlesegerätes mit eigenem Nummernfeld für die Eingabe der Geheimnummer. Unbedingt notwendig ist in jedem Fall die eigentlich selbstverständliche Absicherung des heimischen PCs. Dazu zählt der Einsatz eines aktuellen Virenscanners und einer Firewall. Weiterhin sollte der PC ohne Administratorrechte genutzt werden.

Anbieter im Internet brauchen zur Kommunikation mit Bürgerinnen und Bürgern im Internet sog. Berechtigungszertifikate, die sie beim Bundesverwaltungsamt beantragen müssen. Darin ist festgelegt, welche Daten aus dem neuen Personalausweis ausgelesen werden dürfen. Dazu müssen Antragstellende vorher die Erforderlichkeit dieser Daten für ihren Dienst nachweisen. Möchte jemand einen Dienst im Internet mit der eID-Funktion nutzen, muss sie oder er den neuen Personalausweis auf das Lesegerät legen und die entsprechende Internetseite des Händlers auswählen. Sie oder er gibt die PIN ein und bekommt im Gegenzug das Berechtigungszertifikat des Händlers angezeigt. Der Nutzerin oder dem Nutzer wird nun die Möglichkeit gegeben zu entscheiden, welche Daten vom Personalausweis wirklich an den Händler übertragen werden sollen. Die Übertragung der Daten erfolgt verschlüsselt. Es wird auch die zuständige Datenschutzaufsichtsbehörde angezeigt, an die man sich im Streitfall wenden kann. Dies erleichtert das Einreichen von Beschwerden, wenn Diensteanbieter Daten zweckentfremdet verwenden sollten.

Sehr zu befürworten ist die **Möglichkeit der pseudonymen Nutzung** des neuen Personalausweises im Internet. Ist die Kenntnis der wahren Identität der Nutzenden nicht notwendig, kann mit jedem Internetanbieter automatisch ein gesonderter Codename vereinbart werden, der bei jeder Nutzung beim gleichen Anbieter wiederverwendet wird. Die Übermittlung des wirklichen Namens ist hierbei nicht notwendig. Sind bei diesem Dienst Geldbeträge zu überweisen, kann dies natürlich nur mit anonymen Zahlverfahren kombiniert werden. Da bei jedem Internetanbieter ein eigenes Pseudonym verwendet wird, sind anbieterübergreifende Nutzerprofile aus technischer Sicht nicht möglich.

Auch kann der neue Personalausweis zur Verifikation des Alters und des Wohnorts im Internet eingesetzt werden. Möchte man z. B. Internetseiten mit einer bestimmten Altersbeschränkung besuchen, kann abgefragt werden, ob die Inhaberin oder der Inhaber des Ausweises ein gewisses Alter, z. B. 18 Jahre, erreicht hat. Möchte man Leistungen in Anspruch nehmen, die nur im Bereich eines Ortes angeboten werden, kann man den Ort abfragen. Die Übermittlung des Geburtsdatums oder der Adresse ist dann nicht notwendig, nur die Tatsache, dass ein bestimmtes Alter bzw. ein bestimmter Wohnort vorliegt. Beides ist aus Gründen der Datensparsamkeit sehr zu begrüßen.

Die zweite neue elektronische Funktion des neuen Personalausweises ist die optionale Nutzung der **qualifizierten elektronischen Signatur (QES)**. Die QES-Anwendung soll eine sichere, rechtsverbindliche und signaturgesetzkonforme elektronische Unterschrift ermöglichen. Der neue Personalausweis bietet damit die gleichen Funktionen wie bereits bekannte Signaturkarten. Diese Funktion ist bei Abholung des Ausweises nicht sofort nutzbar. Für die Nutzung der QES-Funktion muss ein käuflich zu erwerbendes Zertifikat bei entsprechenden Diensteanbietern nachgeladen werden. Die Nachlademöglichkeit eines qualifizierten Signaturzertifikats ermöglicht es den Inhaberinnen und Inhabern des neuen Personalausweises, eine Zertifizierungsstelle ihrer Wahl auszusuchen. Sie müssen aber den Verlust des Ausweises nicht nur der ausgebenden Behörde melden, sondern auch ihrer Zertifizierungsstelle, da dies nicht automatisch erfolgt.

Eine wichtige Änderung betrifft auch die **Praxis des Hinterlegens von Personalausweisen**. Da der neue Personalausweis über neue wesentliche elektronische Funktionen verfügt, darf nicht mehr verlangt werden, den Personalausweis zu hinterlegen. Dies bedeutet, dass ein Hotel den Personalausweis beim Einchecken nicht mehr einbehalten darf.

Geht der neue Personalausweis verloren, muss dies umgehend der ausstellenden Behörde mitgeteilt werden. Diese sperrt den Ausweis und damit die zusätzlichen neuen Funktionen (wenn man sich für ihre Nutzung entschieden hatte). Es kommt aber auch immer wieder vor, dass gültige Personalausweise in einer Personalausweisbehörde abgegeben werden, weil sie entweder nach Verlust oder Diebstahl aufgefunden wurden oder weil die Ausweisinhaberin bzw. der Ausweisinhaber verstorben ist. Falls nun eine Mitarbeiterin oder ein Mitarbeiter

dieser Behörde die PIN ändert, kann es zu einem **Missbrauch der eID-Funktion** im Internet kommen. Selbst wenn die eID-Funktion nicht aktiviert war, könnte sie dann aktiviert werden. Ein Mitwirken der Ausweisinhaberin oder des Ausweisinhabers ist hier nicht vorgesehen. Bisher sehen weder die personalausweisrechtlichen Vorschriften noch die eingesetzte Technik ausreichende Sicherheitsmaßnahmen zur Behebung dieses Problems vor. Um eine unbefugte Neusetzung der PIN in einer Personalausweisbehörde zu verhindern, müssten die Ausweisinhaberinnen und -inhaber aktiv beteiligt werden können.

Der neue Personalausweis kann auch nur ein normaler herkömmlicher Personalausweis sein, wenn man seine neuen zusätzlichen Funktionen nicht nutzen möchte. Möchte man diese elektronischen Funktionen im Internet nutzen, sollte man einen Komfortkartenleser einsetzen, der über ein eigenes Eingabefeld für die Geheimnummer verfügt. Der verwendete PC sollte immer auf dem neuesten Sicherheitsstand gehalten werden. Dazu gehört ein aktueller Virenscanner, eine Firewall und alle Sicherheitsupdates des Betriebssystems. Das Problem der unbefugten Aktivierung der eID-Funktion durch Bedienstete einer Personalausweisbehörde muss noch gelöst werden.

2.5 Smartphone-Apps – wo bleibt der Datenschutz?

In den letzten Jahren haben sich die sog. Smartphones stark verbreitet. Das sind mobile Geräte, die neben der obligatorischen Telefoniefunktion aufgrund größerer Displays, steigenden Speicherplatzes und verbesserter Rechenleistung sowie wegen der Verbreitung von bezahlbarem und schnellem mobilem Internet wesentlich weiter gehende Nutzungen ermöglichen. Nahezu klassische Anwendungen sind dabei Adressbuch und Kalender, die mobile Internet- und E-Mail-Nutzung, das Abspielen von Audio- und Videodateien, Aufnehmen von Fotos und Videos sowie Versenden von Kurznachrichten.

Im Gegensatz zu früheren Versuchen, das Internet auf mobilen Endgeräten nutzbar zu machen (z. B. das WAP-Protokoll) werden heute häufig normale Webseiten auf Smartphones angezeigt – für die Darstellung auf kleinen Displays ggf. mit beschränktem Inhalt. Da diese Lösung nicht optimal ist, wurden

die sog. „Smartphone-Apps“ erfunden. Dies sind kleine Programme („Applications“, Anwendungen), die, auf dem Smartphone installiert, den Nutzenden bestimmte Funktionalitäten zur Verfügung stellen. Unterscheiden kann man Apps, die wie konventionelle Computerprogramme ausschließlich auf dem Smartphone arbeiten. Beispiele wären ein elektronischer Einkaufszettel oder diverse Spiele. Die Mehrheit der Apps nutzt jedoch die Internetverbindung, um interessantere oder produktivere Dienstleistungen zur Verfügung stellen zu können. So könnte sich ein Einkaufszettel mit denen der anderen Haushaltsmitglieder automatisch synchronisieren, oder man könnte gegen oder mit anderen Nutzenden spielen. Viele Apps nutzen die Ortung der aktuellen Position, gespeicherte (Kontakt-)Daten, Nahfunktechniken wie Bluetooth sowie die von den Geräten zur Verfügung gestellten Sensordaten wie Lage- und Bewegungsdaten, Bild und Ton.

Entwickelt und angeboten werden die Apps mehrheitlich nicht von dem Hersteller des jeweiligen Smartphones, sondern von Dritten. Üblicherweise stellt zudem der Hersteller des Smartphones einen sog. App-Store („Marktplatz“) zur Verfügung, in welchem alle verfügbaren Apps zum unkomplizierten, teilweise kostenpflichtigen Download angeboten werden.

Datenschutzprobleme vernetzter Smartphone-Apps

Die weite Verbreitung von Smartphones und den darauf installierten (und potentiell ständig aktiven) Apps führt zu Datenschutz- und Sicherheitsproblemen, die teilweise schon aus dem Bereich der stationären Computer bekannt sind. Durch die besonderen Eigenschaften von Smartphones kommen jedoch auch neue Gefahren hinzu oder es verschärfen sich bekannte Gefahren.

Ein Problem ist die Kombination aus permanentem Internetzugang und der Fähigkeit, auf Daten zuzugreifen, die auf dem Smartphone gespeichert sind oder die über die verfügbaren Sensoren ermittelt werden können. Es ist sehr schlecht kontrollierbar, was eine App mit diesen Daten neben der Erfüllung des eigentlichen Zwecks der Anwendung tut. Ein Beispiel für eine solche Datenverarbeitung ist das zunehmende Angebot von mobiler Werbung. Ebenso wie bei Webangeboten gilt mobile Werbung als besonders effektiv, wenn sie auf die Interessen der Nutzenden und ihre aktuelle Situation zugeschnitten wird. Bei mobilen Geräten ist ein wesentlicher Punkt der Ortsbezug: Um für die Pizzeria

um die Ecke werben zu können, werden bereits jetzt von vielen Apps regelmäßig GPS-Koordinaten sowie weitere Daten wie eine Gerätenummer an den Server des Werbedienstleisters gemeldet.

Neben dieser grundsätzlich legitimen Datennutzung haben Studien gezeigt, dass ein erheblicher Teil der Apps verschiedene personenbezogene Daten (wie Gerätenummer, Telefonnummer, Kontaktdaten aus dem Adressbuch) an den jeweiligen App-Hersteller übermittelt, ohne dass dies für den jeweiligen Dienst erforderlich wäre und ohne die Nutzenden zu informieren.

Zur Ermittlung der aktuellen Position wird längst nicht nur GPS benutzt. Dies ist zwar die genaueste Methode, aber z. B. in Gebäuden nicht immer verfügbar. Zudem gibt es viele Geräte, die nicht über einen GPS-Chip verfügen. Andere Methoden zur Positionsermittlung sind WLAN-Accesspoints und die Funktürme der Mobilfunknetze: Jede Station besitzt eine weltweit eindeutige Kennnummer. Es gibt spezialisierte Dienstleister, die in umfangreichen Datenbanken die Standorte (GPS-Koordinaten) solcher Stationen vorhalten. Ein Smartphone ermittelt also seine Position, indem es die Kennnummern der Stationen in Reichweite an diesen Dienstleister sendet, der im Gegenzug den Aufenthaltsort zurückmeldet. Dies tun aber viele Smartphones auch dann, wenn die Position datensparsam per GPS ermittelt wurde, damit die Datenbank die Positionen neuer Stationen kennenlernt.

Bei jeder Nutzung einer App, die den Aufenthaltsort verwendet, erfahren also potenziell der Lokalisierungs-Dienstleister, der Hersteller des Smartphone-Betriebssystems, der Landkarten-Dienstleister, der App-Hersteller, der Werbedienstleister und natürlich der Mobilfunk-Netzbetreiber zumindest ungefähr die jeweils aktuelle Position des Smartphones, selbst wenn das für das jeweilige Angebot oder die Anwendung nicht erforderlich ist. Einige dieser Dienstleister haben ihren Sitz nicht in der EU, sodass sie auch nicht an europäische Datenschutzbestimmungen gebunden sind. Zudem erfahren einige Dienstleister noch wesentlich mehr: Eine eindeutige Gerätekennung ist fast allen zugänglich. Damit ist es möglich, einzelne Aufenthaltsorte zu einem Bewegungsprofil zusammenzusetzen. Handelt es sich um eine „soziale App“, d. h. einen mobilen Zugang zu einem sozialen Netzwerk, erfahren die Anbieter zudem Daten über die Person der oder des Nutzenden (wie Alter, Geschlecht) und den Freundeskreis. Da Smartphones im Wesentlichen immer aktiv sind und ständig mitge-

führt werden, entstehen leicht **umfangreiche Interessens- und vollständige Bewegungsprofile.**

Datenschutzrelevant können auch bestimmte Funktionalitäten von Apps sein. Als Beispiel soll hier die Fähigkeiten zur Bilderkennung genannt werden. Die App Goggles der Suchmaschine Google kann seit kurzem Objekte auf einem Foto identifizieren. Bisher ist die Identifizierung (Gesichtserkennung) von Personen bei der Fotosuche aus Datenschutzgründen abgeschaltet. Neuere Forschungen zeigen aber, dass das Profil einer fotografierten Person in einem sozialen Netzwerk technisch bereits jetzt leicht zu finden ist.

Zentrale Position des Plattformanbieters

Ein wesentlicher Unterschied zwischen PC und Smartphone ist die Stellung des Plattformanbieters. Üblicherweise werden die Apps über einen zentralen, vom Plattformbetreiber kontrollierten Dienst, den sog. AppStore, installiert. Der AppStore ermöglicht dem Plattformbetreiber die Kontrolle über die auf der Plattform eingesetzten Anwendungen. Einerseits ist dies aus Sicherheits- und manchmal auch aus Datenschutzgesichtspunkten gut, da es dadurch eine unterschiedlich umfangreiche „Zugangskontrolle“ gibt, die zumindest prinzipiell gefährliche und besonders datenhungrige Anwendungen von der Plattform fernhalten kann. Leider macht man sich dabei von den Kriterien eines privaten Unternehmens abhängig. Andererseits erfährt der Plattformbetreiber so auch besonders viel über die Nutzenden – jede Installation, ggf. auch jede Nutzung einer App – und speichert diese Daten beispielsweise für Abrechnungszwecke.

Rechtliche und technische Schutzmaßnahmen

Bisher gibt es nur begrenzte Möglichkeiten des Selbstschutzes. Teilweise können die Rechte von Apps beschränkt werden. So kann man festlegen, ob eine App auf die Lokalisierungsfunktionalität zugreifen darf. Manche Plattformen schränken den Datenzugriff von Apps grundsätzlich ein. Bei anderen erbittet eine App bei der Installation die notwendigen Rechte. Problematisch ist hierbei, dass sich die Anwendungsentwickler oft zu umfangreiche und nicht notwendige Rechte geben lassen. Der Effekt ist folgender: Die Mehrheit der Nutzenden gewährt die geforderten Rechte ungeprüft, da ansonsten die jeweilige Anwendung nicht arbeitet. Zudem können die Nutzenden kaum überprüfen,

ob eine Anwendung bestimmte Rechte ausschließlich zu den vorgesehenen Zwecken nutzt.

Aus rechtlicher Sicht ist gegenwärtig – solange es keine internationalen Vereinbarungen und verbindlichen Standards gibt – ebenfalls kaum eine Lösung in Sicht, insbesondere wenn Apps von Anbietern außerhalb der EU angeboten werden oder Funktionalitäten wie die oben beschriebene Lokalisierung genutzt werden, die auf Dienstleister in Ländern außerhalb des Europäischen Wirtschaftsraumes, z. B. in den USA, zurückgreift.

Vernetzte Smartphone-Dienste bergen immer die Gefahr, dass personenbezogene Daten Dritten zugänglich werden. Bei Installation einer App ist deshalb Vorsicht geboten: Gründliches Informieren über das Angebot, Lesen der jeweiligen Allgemeinen Geschäftsbedingungen und Datenschutzerklärungen sind Pflicht. Eine App sollte nur die Rechte erhalten, die sie für ihr Funktionieren nachvollziehbar benötigt.

2.6 Tracking im Internet – Europa will den Schutz verbessern

In den letzten Jahren hat sich das Internet und insbesondere das World Wide Web stark gewandelt. Eine aktuelle Webseite ist kein statisches Informationsdokument mehr, welches von dem Anbieter an alle Nutzenden identisch ausgeliefert wird, sondern setzt sich aus vielen einzelnen Objekten zusammen, die sich dynamisch verändern können und u. U. individuell an die Interessen der jeweiligen Lesenden angepasst werden. Zudem können die einzelnen Objekte von verschiedenen Anbietern stammen, ohne dass dies den Lesenden auffallen muss.

Ein Beispiel für sich derartig anpassende Webseiten ist das Angebot eines bekannten Internet-Buchhändlers. Schon die Startseite zeigt Empfehlungen, die aufgrund des bisherigen Kaufverhaltens automatisch ausgewählt werden. Bei Auswahl eines Artikels werden weitere Artikel vorgeschlagen, beispielsweise auf Basis des Verhaltens anderer Käuferinnen und Käufer des Artikels. Andere Webangebote finanzieren sich hauptsächlich durch Werbung, die wesentlich

effektiver ist, wenn Produkte und Dienstleistungen empfohlen werden, die den jeweiligen Lesenden vermutlich interessieren könnten. Besonders relevant ist die Personalisierung von Inhalten und auch Werbung auf mobilen Endgeräten, da auf diesen der verfügbare Platz wegen der kleinen Displays begrenzt ist.

Personalisierung ist nur möglich, wenn der die Webseite ausliefernde Server Informationen über die jeweils Zugreifenden besitzt. Bei manchen Diensten wie z. B. sozialen Netzwerken geben die Nutzenden Informationen wie Alter, Geschlecht und auch Interessen in eigenen Profilen freiwillig an. Rein technisch können diese Daten problemlos dafür genutzt werden, passende Werbung auszuwählen. Bei anderen Webangeboten ist eigentlich nichts über die Zugreifenden bekannt, abgesehen davon, dass der Inhalt der Seite offensichtlich deren Interesse geweckt hat. Wer nun die Aktivitäten von Nutzenden (auf verschiedenen Webangeboten) über eine längere Zeit beobachtet, erfährt ziemlich genau, für welche Themen sich die Person interessiert, und kann daraus auch auf andere persönliche Daten wie Geschlecht, Altersgruppe sowie sonstige für die Werbeindustrie wichtige Kenngrößen wie Kaufkraft und Lebenssituation schließen.

Der neueste Hype ist derzeit das sog. **„Re-Targeting"**. Dies bedeutet, dass Nutzende, die einen bestimmten Webshop besuchen, aber vielleicht noch nicht gekauft haben, auf anderen Webseiten ganz speziell ausgewählte Werbung dieser Webshops gezeigt bekommen – beispielsweise genau das Produkt, für welches sie sich interessiert haben, vielleicht mit einem zusätzlichen Rabatt. Man bleibt dadurch auch dann im Visier des hartnäckigen Verkäufers, wenn man dessen Webseite längst verlassen hat.

Technisch wird zum langfristigen Erfassen der Aktivitäten einer bzw. eines Nutzenden der sog. **Cookie-Mechanismus** eingesetzt. Dabei weist die Webseite den Browser an, auf dem jeweiligen Computer eine kleine Datei abzuspeichern und bei jedem weiteren Besuch der Webseite dem Server die darin gespeicherten Daten wieder mitzuteilen. In den meisten Fällen handelt es sich dabei um eine kurze Identifikationsnummer (Kundennummer), die auf eine Datenbank bei dem Anbieter verweist. In dieser Datenbank speichert der Anbieter nun alles, was er über die Nutzerin oder den Nutzer bereits in Erfahrung gebracht hat, und verwendet die Daten, um das Webangebot oder die eingeblendete Werbung anzupassen. Im Fall des Internetbuchhändlers können die angepassten

Empfehlungen ganz nützlich sein. Allerdings tut der Anbieter dies hauptsächlich, um seinen Umsatz zu erhöhen. Problematisch ist in jedem Fall, dass dafür sehr detailliert gespeichert wird, zu welchen Themen jemand Bücher gekauft oder auch nur angeschaut hat.

Die rechtliche Situation ist hierbei eindeutig: Eine personenbezogene Speicherung von Nutzungsdaten darüber, welche Seiten eines Internetangebotes sich jemand angesehen hat (der Buchhändler kennt zudem Namen und Adresse), ist nur nach Einwilligung zulässig. Nicht ganz so eindeutig ist die Situation, wenn der Anbieter nur eine Reihe von Interessensdaten beobachtet, ohne die Betroffenen zu identifizieren. Hier spricht man von einer **Datensammlung unter Pseudonym.**

Für eine solche Datensammlung unter Pseudonym fordert das Telemediengesetz bisher nur die Information der Betroffenen sowie die Einräumung einer Möglichkeit zum Widerspruch. Werberinge berufen sich auf diese Vorschrift: Ihre Betreiber haben Verträge zur Einblendung von Werbung mit tausenden unterschiedlichen Webangeboten. Die Werbebanner auf den jeweiligen Angeboten werden dabei direkt von Servern des Werberinges geladen und es werden Cookies bzw. ähnliche Techniken verwendet, um die Nutzenden auf jedem Webangebot wiederzuerkennen und auf diese Weise möglichst umfangreiche Profile erstellen zu können. Da auf dem Server des Werberinges nur die Interessen unter einer Identifikationsnummer geführt werden, sollen die Daten pseudonym oder nach der nicht zutreffenden Meinung mancher Anbieter gar anonym sein.

Das Problem mit Datensammlungen auf Basis von Cookies ist, dass die **Nutzenden** darüber oft **nicht ausreichend informiert** werden. So hat kaum jemand eine Vorstellung, wie detailliert solche Profile werden können, über welchen Zeitraum sie gespeichert werden und welche Schlussfolgerungen die Betreiber aus diesen Daten ziehen. Die höchste Transparenz bietet nach Interventionen der Datenschutzbeauftragten diesbezüglich noch das Adwords-System von Google: Neben jeder Werbeanzeigengruppe gibt es einen Link, der zu einer Informationsseite führt, die zumindest die vom System ermittelten Interessen aufführt und eine Widerspruchsmöglichkeit direkt anbietet. Andere Anbieter geben den Nutzenden keinerlei Informationen über die konkret gespeicherten Daten oder wenigstens über den Umfang des Netzwerkes. Bes-

tenfalls findet man die gesetzlich vorgeschriebene Widerspruchsmöglichkeit in einer technisch problematischen Realisierung: Die Betreiber bieten an, einen Opt-Out-Cookie zu setzen, der dem Dienstleister signalisiert, dass kein Profil gespeichert werden soll. Allerdings erfolgt die Auswertung des Opt-Out-Cookies erst nach der Datenübermittlung an den Server des Werbeanbieters, der ja gerade widersprochen wurde. Zudem wird ein Opt-Out-Cookie beim empfehlenswerten regelmäßigen Löschen der Cookies mit gelöscht. Die essenzielle **Information der Betroffenen** über Datenerhebung und Widerspruchsmöglichkeiten wird regelmäßig **auf die Betreiber der Webangebote abgewälzt,** die diese oft nicht in ausreichendem Maße erfüllen, beispielsweise nur allgemein von der Zusammenarbeit mit Ad-Servern sprechen, aber nicht den konkreten Anbieter nennen.

Besonders problematisch ist, dass die Datensammlungen webseitenübergreifend erfolgen. Im schlimmsten Fall werden alle von einer oder einem Nutzenden besuchten Webangebote über Jahre protokolliert. Je umfangreicher ein solches **Verhaltensprofil** wird, desto sensitiver sind die gespeicherten Daten und desto höher ist zudem die Wahrscheinlichkeit, dass sich doch eine Möglichkeit zur Identifizierung ergibt. Suchmaschinen beispielsweise protokollieren eingetippte Suchworte. Da die durchgeführte Suche nicht selten etwas mit der eigenen Person oder dem Freundeskreis zu tun hat, konnten aus einer versehentlich veröffentlichten anonymisierten Liste von Suchanfragen einzelne Personen identifiziert werden[93]. Potenziell liegen für alle Internetnutzenden bei den Betreibern großer Werberinge und der Suchmaschinen personenbeziehbare Interessen-Dossiers vor.

Mittlerweile hat sich herumgesprochen, dass man Cookies von solchen Drittanbietern am besten nicht akzeptiert und sowieso die von Browsern gespeicherten Cookies regelmäßig löschen sollte. Manche Webbrowser bieten derweil komfortabel nutzbare datenschutzfreundliche Einstellungsmöglichkeiten (leider jedoch nicht als Voreinstellung). Einige Anbieter versuchen daher andere Speicherorte zu nutzen, die den Nutzenden noch unbekannt sind und sich zudem nicht bzw. nicht so leicht löschen lassen. Inzwischen gibt es dafür eine ganze Reihe „Verstecke“ wie das Flash-Plugin, neuere Erweiterungen von HTML oder auch eine geschickte Nutzung des Browserverlaufs bzw. der lokal zum

93 http://ct.de/-165698

schnelleren Laden einer Webseite gespeicherten Cache-Daten. Das kleinste Problem ist dabei noch der höhere mögliche Speicherplatz: Zum Verfolgen der Nutzenden genügt das Ablegen einer kurzen Identifikationsnummer. Im Gegenteil: Der größere verfügbare Speicherplatz könnte im Prinzip genutzt werden, um die Internet-Werbung datenschutzfreundlicher zu machen, einfach indem die für personalisierte Werbung nötigen Profildaten nur lokal unter Nutzerkontrolle gespeichert und ausgewertet werden. Bisher ist eine solche Entwicklung jedoch nicht zu beobachten.

Aber auch ohne die **geheime Speicherung von Identifikationsnummern** auf den Computern der Nutzenden bestehen Möglichkeiten der Wiedererkennung der Nutzenden: Jeder Browser sendet mit einer Anfrage eine größere Anzahl von Informationen zum Server. Der Zweck ist, beispielsweise die Webseite in der richtigen Sprache oder eine für Mobilgeräte angepasste Seite auszugeben. Diese Informationen sowie andere Daten über das Endgerät, die eine Webseite anderweitig (oft per JavaScript) ermitteln kann, ergeben zusammengenommen einen ziemlich individuellen **„Fingerabdruck“ des Rechners,** wie die US-Organisation Electronic Frontier Foundation zeigen konnte[94].

Datenschutzrechtliche Bewertung

Das Telemediengesetz schreibt eine informierte Einwilligung bei der Sammlung personenbezogener Daten vor. Kann der Datensammler nachweisen, dass ein direkter Personenbezug nicht hergestellt wird, die Datensammlung also nur unter einem Pseudonym erfolgt, genügt es derzeit, die Nutzenden umfassend zu informieren und ihnen ein Widerspruchsrecht einzuräumen. Allerdings muss die Gesetzeslage an die im Dezember 2009 g**eänderte europäische E-Privacy-Richtlinie (2002/58/EG)**[95] angepasst werden, die auch im Falle pseudonymer Datensammlungen auf Basis von Daten, die auf den Rechner der Nutzenden gespeichert sind, eine **informierte Einwilligung** der Betroffenen vorschreibt.

Dies ist in jedem Fall eine Herausforderung für die Internet-Werbewirtschaft und erfordert u. U. auch eine Umstellung bestimmter Geschäftsmodelle. Allein die Browser-Konfiguration zur Annahme von Cookies erfüllt die For-

94 http://ct.de/-1002375
95 Vgl. Dokumentenband 2010, S. 34

derung nach einer informierten Einwilligung keinesfalls. Eine technische Lösung könnte die **Erweiterung des Cookie-Mechanismus** sein, die neben der Abfrage zur Speicherung eines Cookies im Einzelfall auch Angaben zu dem Verarbeitungszweck, der verantwortlichen Stelle sowie den technischen Möglichkeiten zum Zurückziehen der Einwilligung beinhaltet. Jedenfalls unzulässig sind die oben skizzierten Methoden, die Entscheidung der Betroffenen gegen Cookie-gestützte Werbung durch andere Speichertechniken wie Flash-Cookies oder durch Auswertung der zu anderen Zwecken übermittelten Browserdaten zu umgehen.

Selbstschutz

Da die geänderte E-Privacy-Richtlinie noch nicht in nationales Recht umgesetzt ist und zudem der Markt für Internetwerbung von Firmen dominiert wird, die ihren Sitz nicht in der EU haben, zählen wir im Folgenden einige Möglichkeiten zum Selbstschutz auf:

1. Konfigurieren Sie Ihren Browser so, dass Cookies nur von der aufgerufenen Seite akzeptiert werden (keine Cookies von Dritten wie Werberingen akzeptieren).
2. Konfigurieren Sie Ihren Browser so, dass die Cookies regelmäßig gelöscht bzw. grundsätzlich nur während der aktuellen Sitzung gespeichert werden. Ggf. können Sie Ausnahmen für einzelne vertrauenswürdige Seiten definieren.
3. Lassen Sie regelmäßig den Verlauf und den Cache Ihres Browsers löschen und deaktivieren Sie den lokalen Speicher des Flashplayers[96].
4. Manche Browser erlauben, die Ausführung aktiver Inhalte zu blockieren und wenn nötig seitenspezifisch freizuschalten. Auch können Webadressen bekannter Trackingdienste gesperrt werden. Für Firefox sind diesbezüglich beispielsweise folgende kostenlose Addons empfehlenswert: Ghostery, Adblock-Plus und Noscript.

96 Adobe Einstellungsmanager: http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html

Der gläserne Surfer ist im Internet längst Realität geworden. Private Firmen protokollieren, wenn die Einzelnen sich nicht wehren, fast jeden Schritt im Netz, um angepasste Werbung zu zeigen. Verbessern kann sich dieser Zustand nur, wenn die überarbeitete E-Privacy-Richtlinie sowohl national als auch international umgesetzt wird und die Nutzenden sensibilisiert werden.

3. Öffentliche Sicherheit

3.1 Körperscanner

Aus der Praxis

Die Diskussion um den Einsatz von sog. Körperscannern bei Passagierkontrollen am Flughafen hat durch den Anschlagsversuch in Detroit Ende 2009 eine Eigendynamik entwickelt. Auf europäischer Ebene ist beabsichtigt[97], den Körperscanner bei Personenkontrollen zuzulassen. Dabei handelt es sich um Geräte, mit denen der Körper einer Person sowie Gegenstände unter der Kleidung abgebildet werden. So können am Körper getragene Waffen und Sprengstoff sichtbar gemacht werden. Mit dieser Technik sollen Sicherheitslücken geschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zunächst eine Klärung der Frage gefordert, ob vor dem Hintergrund der ernsthaften Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie mit solchen Geräten ein nennenswerter Sicherheitsgewinn erzielt werden kann.[98]

Ferner muss sichergestellt sein, dass die beim Einsatz von Körperscannern erhobenen Daten der Kontrollierten einschließlich der erstellten Bilder über den Scanvorgang hinaus nicht gespeichert werden. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel wie Prothesen und künstliche Darmausgänge dürfen nicht angezeigt werden. Der Nachweis, dass diese Bedingungen erfüllt sind, ist in praktischen Tests und Erprobungen zu erbringen.

97 Entwurf einer Verordnung zur Ergänzung der im Anhang der Verordnung (EG) Nr. 300/2008 (ABl. L 97 vom 9. April 2008, S. 72) festgelegten gemeinsamen Grundstandards für die Sicherheit der Zivilluftfahrt (Ratsdok. 12815/08)

98 Entschließung vom 17./18. März 2010: Körperscanner – viele offene Fragen, Dokumentenband 2010, S. 9; vgl. auch die Entschließung der Europäischen Datenschutzkonferenz vom 29./30. April 2010: Einsatz von Körperscannern für die Sicherheit an Flughäfen, Dokumentenband 2010, S. 30

Auf dem Hamburger Flughafen wird seit dem Herbst in einem Feldversuch der Einsatz des Körperscanners getestet. Die Daten werden nach dem Scanvorgang nicht gespeichert. Es erfolgt lediglich eine statistische Aufzeichnung über die Zahl der detektierten Personen und die Alarmmeldungen. Windeln, Katheter sowie künstliche Darmausgänge werden allerdings bei der Kontrolle detektiert und in schematischen Darstellungen der Körperumrisse angezeigt. Das Ergebnis des Feldversuches und die weitere Entwicklung bleiben abzuwarten.

Bei der Einführung neuer Technologien ist nicht nur auf den Sicherheitsgewinn abzustellen, sondern auch darauf zu achten, dass die Grundrechte der Betroffenen nicht verletzt werden und insbesondere ihre Menschenwürde geachtet wird.

3.2 Nationales Waffenregister

Aus der Praxis

Der Aufbau eines bundesweit einheitlichen und computergestützten Waffenregisters ist als neues Vorhaben mit hoher Priorität in den Aktionsplan Deutschland Online aufgenommen worden.

Durch eine Änderung der europäischen Waffenrichtlinie vom Mai 2008[99] sind die EU-Mitgliedstaaten verpflichtet, bis Ende 2014 ein computergestütztes Waffenregister einzuführen und darin mindestens für 20 Jahre alle Schusswaffen mit den Angaben über Typ, Modell, Fabrikat, Kaliber, Seriennummer, Name und Anschrift des Verkäufers und des Waffenbesitzers zu erfassen. Daneben werden die Voraussetzungen geschaffen, um die bei derzeit ca. 570 Waffenbehörden auf Basis unterschiedlichster Software oder in Einzelfällen noch per Karteikarte erfassten Informationen aufzubereiten und in ein abgestimmtes computergestütztes System zu überführen.

Das Nationale Waffenregister ist datenschutzrechtlich nicht unproblematisch. So haben wir erhebliche Zweifel hinsichtlich des lesenden Zugriffs der Innenministerien in Bund und Ländern, der Zoll- und Verfassungsschutzbehörden

99 2008/51/EG

sowie bezüglich der für den Bundesnachrichtendienst und den Militärischen Abschirmdienst vorgesehenen Zugriffsrechte. Der Fortgang der Angelegenheit – insbesondere das geplante Errichtungsgesetz – bleibt abzuwarten.

Der Zugriff auf das Nationale Waffenregister ist datenschutzkonform zu regeln.

3.3 Schiffskontrolldatei – eine Verbunddatei ohne Rechtsgrundlage

Die Berliner Wasserschutzpolizei betreibt wie fast alle anderen Wasserschutzpolizeien der Länder ihre eigene Schiffskontrolldatei. Damit soll u. a. der Fahndungsdienst unterstützt, unnötige Mehrfachkontrollen mit der damit verbundenen Behinderung der gewerblichen Schifffahrt vermieden sowie die Behebung von bei Kontrollen festgestellten Mängeln überwacht werden. Sie dient der Abwehr von Gefahren für die Sicherheit und Leichtigkeit des Verkehrs sowie der Verhütung von schifffahrtsbedingten Gefahren und schädlichen Umwelteinwirkungen.

Seit zwei Jahren streben die Wasserschutzpolizeien nahezu aller Bundesländer eine gemeinsame Nutzung der von Rheinland-Pfalz entwickelten und beim dortigen „Landesbetrieb Daten und Informationen“ zentral betriebenen Schiffskontrolldatei, wobei dieser Landesbetrieb als Auftragnehmer tätig sein soll.

Dem Wesen nach handelt es sich bei der Datei um eine Verbundanwendung. Die einschlägigen Regelungen des Bundeskriminalamtsgesetzes sind allerdings nicht anwendbar, das Binnenschifffahrtsaufgabengesetz enthält keine ausreichenden Regelungen zur Verarbeitung personenbezogener Daten. Aus diesem Grund wird das Verfahren als Auftragsdatenverarbeitung konzipiert.

Der Charakter der Auftragsdatenverarbeitung bleibt vor allem dadurch erhalten, dass Änderungen an den Daten nur von den Ländern vorgenommen werden können, die die Daten auch eingestellt haben. Ferner gehen wir davon aus, dass

die bisher vorliegende Generalerrichtungsanordnung für das Verfahren auf die Wasserschutzpolizei Rheinland-Pfalz zugeschnitten ist und jede teilnehmende Wasserschutzpolizei ihrerseits eine eigene Errichtungsanordnung schafft.

Die geplante Auftragsdatenverarbeitung in Rheinland-Pfalz schafft aber noch keine Rechtsvorschrift für die Übermittlung von Daten an andere Polizeibehörden. Die Berliner Polizei kann mit anderen Ländern und dem Bund einen Datenverbund vereinbaren, der eine automatisierte Datenübermittlung ermöglicht.[100] Voraussetzung dafür ist allerdings der Erlass einer Rechtsverordnung. Dabei sind die Datenempfänger, die Datenart und der Zweck des Abrufs festzulegen und Maßnahmen zur Datensicherung und Kontrolle vorzusehen. Die Senatsverwaltung für Inneres und Sport hat uns schon 2006 den Entwurf einer Verordnung über den automatisierten Datenabruf aus der Schiffskontrolldatei vorgelegt. Inzwischen beschäftigt sich der Unterausschuss Recht und Verwaltung der Innenministerkonferenz mit dem Thema. Konkrete Ergebnisse liegen uns noch nicht vor.

Wenn eine Verbundanwendung über die Konstruktion einer Auftragsdatenverarbeitung geschaffen werden soll, sind die dafür vorgegebenen rechtlichen Rahmenbedingungen einzuhalten.

3.4 Evaluationsbericht nach § 70 ASOG

Mit der Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes im Jahr 2007[101] ist nicht nur die Befugnis für die Videoüberwachung zur Eigensicherung[102], zu medizinischen und molekulargenetischen Untersuchungen[103], zur Datenerhebung in öffentlichen Verkehrseinrichtungen[104] sowie zur Standortermittlung bei Telekommunikationsendgeräten[105]

100 § 46 Abs. 5 ASOG
101 GVBl. S. 598 f.
102 § 19 a
103 § 21 a
104 § 24 b
105 § 25 a

geschaffen worden, sondern gleichzeitig wurde der Senat verpflichtet, bis zum 31. Oktober 2010 einen Evaluationsbericht vorzulegen, der Aufschluss über Art und Umfang sowie den Erfolg der jeweiligen Maßnahmen geben soll[106].

Diese Vorschrift enthält (anders als z. B. Art. 11 Terrorismusbekämpfungsgesetz) keine Festlegung, dass wissenschaftliche Sachverständige in die Evaluierung einzubeziehen sind. Dem Bericht ist nicht zu entnehmen, dass er von unabhängigen Wissenschaftlern erstellt oder begleitet worden ist. Es handelt sich offensichtlich um eine Selbsteinschätzung des Senats.

Vor dem Hintergrund der Eingriffsintensität der ASOG-Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Die Evaluation sollte aufgrund valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss für den Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen sein.

In der parlamentarischen Diskussion im Ausschuss für Inneres, Sicherheit und Ordnung bestand im Wesentlichen Einvernehmen darüber, dass die Frist für die Erstellung recht kurz bemessen war. Der Senator für Inneres und Sport hat in der Sitzung (wie von uns vorgeschlagen) zugesagt, fünf Jahre nach dem Inkrafttreten des ASOG-Änderungsgesetzes – also Ende 2012 – eine wissenschaftliche Evaluation durchführen zu lassen.

Eine Evaluation sollte auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Dafür ist eine angemessene Frist vorzusehen.

106 § 70

3.5 Wie umfangreich dürfen Absenderangaben sein?

Ein Bürger ist von der Polizei per Brief zu einem Gespräch eingeladen worden. Der Absenderstempel enthielt neben der Adresse die Angaben „Polizeipräsident in Berlin, Landeskriminalamt, LKA 712 (Hooligan)".

Anders als die Empfängerangaben beispielsweise bei förmlichen Zustellungen nach dem Verwaltungszustellungsgesetz oder der Zivilprozessordnung ist die Absendergestaltung nicht eindeutig geregelt. Somit bemisst sich der Umfang der Angaben am Erforderlichkeitsprinzip[107]. Die Angabe des Absenders ist nur notwendig, um dem Postdienstleister die Rücksendung unzustellbarer Postsendungen zu ermöglichen und den Empfänger, falls nicht ohnehin schon bekannt, in die Lage zu versetzen, etwaige Antwortschreiben richtig und vollständig adressieren zu können. Somit reichen in der Regel der Behördenname, das Stellenzeichen der oder des Beschäftigten und die Adresse (Postleitzahl, Straße, Hausnummer) aus, um nicht zustellbare Postsendungen ungeöffnet der oder dem Beschäftigten zur Entscheidung, wie weiter zu verfahren ist, zuzuleiten. Dem trägt auch die Gemeinsame Geschäftsordnung für die Berliner Verwaltung (GGO I) Rechnung[108]. Danach darf die Absenderangabe nicht mit einem „sprechenden Aktenzeichen" (wie Geburtsdatum der empfangenden Person) oder mit Zusätzen versehen werden, die auf sensible, persönliche oder sachliche Verhältnisse der empfangenden Person schließen lassen (wie „Sozialhilfe", „Geschwulstberatungsstelle" oder „Haftentlassenenhilfe"); wenn erforderlich, ist hier so zu verkürzen oder zu verschlüsseln, dass Rückschlüsse auf persönliche oder sachliche Beziehungen der empfangenden Person nicht möglich sind.

Der Polizeipräsident hat eingeräumt, dass der Zusatz „Hooligan" bei der Absenderangabe nicht erforderlich ist, und angeordnet sicherzustellen, dass die Absenderangabe nicht mehr verwandt wird und alle Dienststellen auf die Regelungen der GGO hingewiesen werden.

Absenderangaben öffentlicher Stellen sind in der Regel auf den Behördennamen einschließlich Stellenzeichen und Adresse zu beschränken.

107 § 9 Abs. 1 BlnDSG
108 § 58 Abs. 5 Satz 2

4. Personenstands- und Ausländerwesen

4.1 Ausführungsverordnung zum Personenstandsgesetz

Aus der Praxis

Mit der Reform des Personenstandsrechts von 2007 wurden die Länder ermächtigt[109], zentrale Register für Standesämter einzurichten, die zur Ausstellung von Urkunden über den Personenstand, zur Erteilung von Auskünften und zur Einsichtsgewährung genutzt werden können.

Die Senatsverwaltung für Inneres und Sport hatte uns den Entwurf einer Ausführungsverordnung des Landes Berlin zum Personenstandsgesetz vorgelegt, nach dessen Wortlaut ein solches zentrales Register eingerichtet werden soll. Diese Verordnung trat gegen Ende des Jahres in Kraft.[110] Dabei ist allerdings offengeblieben, bei welcher Stelle das Register angesiedelt bzw. ob es eine eigenständige öffentliche Stelle ist und welche Verantwortlichkeiten damit verbunden sind. Später wurde uns erklärt, dass – entgegen dem Wortlaut – kein zentrales Register geschaffen werden soll, sondern den Berliner Standesämtern ein gegenseitiges Zugriffsrecht auf die jeweiligen Personenstandsregister und Suchverzeichnisse eingeräumt wird.

Wenn mit der Verordnung ein automatisiertes Abrufverfahren eingerichtet werden sollte, hätte es einer ausdrücklichen Zulassung durch Gesetz bedurft[111]. § 74 Abs. 1 Nr. 3 Personenstandsgesetz, der die Länder ermächtigt, zentrale Register einzurichten, kann dafür nicht herangezogen werden. Ferner sind in der Verordnung die Einzelheiten bei der Einrichtung automatisierter Abrufverfahren festzulegen. So müssen die Datenempfänger, die Datenart und der Zweck des Abrufs bestimmt werden. Auch sind Maßnahmen zur Datensicherung und zur Kontrolle vorzusehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen[112]. Die Rechtsverordnung muss deshalb erheblich

109 § 67 Abs. 1 PStG
110 VO vom 2. November 2010, GVBl. S. 514
111 § 15 Abs. 1 Satz 1 BlnDSG
112 § 15 Abs. 2 BlnDSG

modifiziert werden, bevor der geplante berlinweite Zugriff auf die Register der Standesämter eröffnet werden kann.

Wenn ein zentrales Personenstandsregister in Berlin entstehen soll, dann muss die Verantwortlichkeit für ein solches Register geklärt werden. Sollen dagegen die Standesämter nur zum gegenseitigen Zugriff auf ihre Datenbestände ermächtigt werden, so müssen die Bedingungen dieses automatisierten Abrufverfahrens landesrechtlich festgelegt werden.

4.2 Der elektronische Aufenthaltstitel

Nicht nur die Deutschen erhalten mit dem neuen Personalausweis[113] elektronisch auslesbare Personaldokumente. Die Bundesregierung hat den Entwurf eines Gesetzes zur Anpassung des Rechts zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige eingebracht. Nach einer Verordnung des Rates[114] sind Aufenthaltstitel grundsätzlich als mit biometrischen Merkmalen (zwei Fingerabdrücken und Lichtbild) versehene eigenständige Dokumente auszugeben. Die darüber hinaus vorgesehenen Standards sollen den Schutz vor Fälschungen weiter erhöhen und damit zur Verhinderung und Bekämpfung illegaler Einwanderung und des illegalen Aufenthalts beitragen. Die bisher für Aufenthaltstitel eingesetzten Klebeetiketten werden durch Vollkunststoffkarten in Scheckkartengröße mit einem Datenträger zur Erfassung biometrischer Merkmale ersetzt. Gleichzeitig wird mit dem elektronischen Aufenthaltstitel der Zugang zu neuen Technologien wie elektronischen Behördendiensten oder der digitalen Signatur eröffnet. Die EU-Verordnungen sehen insofern für die Mitgliedstaaten die Möglichkeit vor, den für die Integration biometrischer Merkmale vorgesehenen Datenträger auch zu diesem Zweck zu nutzen. Der Datenträger der elektronischen Aufenthaltstitel wird daher, ebenso wie beim Personalausweis für deutsche Staatsangehörige, technisch so ausgestaltet, dass

113 Vgl. 2.4
114 Verordnung (EG) Nr. 380/2008 des Rates vom 18. April 2008 zur Änderung der Verordnung (EG) Nr. 1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige, ABl. L 115 vom 29. April 2008, S. 1

eine Nutzung zum elektronischen Identitätsnachweis oder zur qualifizierten elektronischen Signatur grundsätzlich möglich ist.

Ferner sollen mit einer Qualitätsverbesserung und Beschleunigung des Datenaustauschs im Ausländerwesen die Voraussetzungen dafür geschaffen werden, künftig einheitliche Standards für den elektronischen Datenaustausch festlegen zu können.

Im Gegensatz zum elektronischen Personalausweis müssen Angehörige von Drittstaaten nach EU-Vorgaben die Aufnahme von Fingerabdrücken in künftige elektronische Aufenthaltstitel hinnehmen. Zugleich soll auch dieser Personenkreis die Möglichkeit erhalten, solche Dokumente zum elektronischen Identitätsnachweis und zur Signatur zu verwenden.

5. Verkehr

5.1 Datenquarantäne bei der Deutschen Bahn AG

Im August haben wir die sog. Quarantäneräume der Deutschen Bahn AG (DB AG) einer datenschutzrechtlichen Kontrolle nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) unterzogen. Diese Räume waren geschaffen worden, um den Datenskandal bei der DB AG straf- und aufsichtsrechtlich aufzuarbeiten, ohne Beschäftigten der DB AG in dieser Phase die Möglichkeit zu geben, auf die Daten zuzugreifen. Ziel unserer Prüfung war es, sich mit Hilfe von Stichproben einen Überblick über die Datenbestände in den Quarantäneräumen, Quarantäneschränken und auf dem Quarantäneserver zu verschaffen. Die Prüfung erstreckte sich auf sämtliche in Berlin vorhandene Quarantäneräume der Revision, der Compliance-Abteilung, der DB Sicherheit und der Rechtsabteilung.

In den Quarantäneräumen befanden sich die Daten, die dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für ihre Prüfungen im Oktober 2008 und Februar 2009 zur Verfügung gestellt wurden. Neben den schon von den Datenschutzbehörden und den Sonderermittlern kontrollierten Vorgängen wurden ab Juli 2009 weitere Datenbestände (Räume, Schränke bzw. Server) unter Quarantäne gestellt. Nach der konzernweiten Anweisung sollten alle Daten, die unzulässig erhoben wurden oder die zunächst zulässig erhoben wurden und deren Zweck für die Speicherung entfallen ist, vollständig in die Datenquarantäne überführt werden.

In der Zeit, in der die Quarantäneräume, -schränke und -server gefüllt wurden, herrschte im DB-Konzern offensichtlich eine große Unsicherheit in datenschutzrechtlichen Fragen. Nur so lässt sich der umfängliche Aktenbestand erklären, den wir im Quarantänebereich vorgefunden haben.

Die weit überwiegende Anzahl der geprüften Akten und Dateien stammte aus unproblematischen Datenverarbeitungsverfahren etwa im Rahmen der Revision und der Compliance-Überprüfung.

Die oben dargestellte Füllung der Quarantäneräume und der dadurch entstandene Aktenumfang trug dazu bei, in der Öffentlichkeit den Verdacht zu nähren, neben den schon untersuchten Vorgängen würden in den Quarantäneräumen weitere Datenskandale verborgen und aufzudecken sein. Dieser Verdacht hat sich nicht bestätigt. Allerdings haben wir bei der Prüfung datenschutzrechtliche Mängel festgestellt, die, soweit noch nicht geschehen, behoben werden müssen. So war insbesondere Folgendes festzustellen:

- Es fehlt im Konzern ein tragfähiges Löschungskonzept, das die gesetzlichen Vorgaben umsetzt.[115] Dies wurde insbesondere bei der Kontrolle der Bewerbungsunterlagen deutlich, die auch nach vielen Jahren noch nicht gelöscht wurden.
- Es wurde im Konzern nicht ausreichend beachtet, dass das Bundesdatenschutzgesetz kein Konzernprivileg enthält. Hier ist ein Konzept für Datenflüsse im Konzern zu entwickeln. Eine entsprechende Betriebsvereinbarung wäre hier sicher hilfreich.
- Schließlich mangelte es an klaren Konzernrichtlinien, ob und ggf. unter welchen Voraussetzungen und zu welchem Zweck medizinische Daten bzw. Diagnosen von Beschäftigten erhoben werden dürfen. Offenbar gab es beim Umgang mit erkrankten Beschäftigten unterschiedliche Verfahrensweisen.

Da die Daten zur Aufarbeitung des Datenskandals nicht mehr benötigt wurden, haben wir die DB AG aufgefordert, sie unverzüglich zu löschen bzw. zu vernichten. Dies ist inzwischen unter unserer Aufsicht geschehen. Die DB AG ist dabei, die genannten datenschutzrechtlichen Mängel zu beseitigen.

In den Quarantäneräumen der DB AG fanden sich keine Anhaltspunkte für weitere Datenskandale.

115 § 35 Abs. 2 Satz 2 Nr. 3 BDSG

5.2 Abfrage des Aufenthaltstitels im Zug

Auf einer Bahnfahrt wurde ein ausländischer Mitbürger von einem Bahnangestellten ohne gültigen Fahrausweis angetroffen. Bei der Datenerhebung für die Fahrpreisnacherhebung beharrte der Bahnangestellte auf der Vorlage des Aufenthaltstitels und teilte dem Fahrgast mit, diese Angabe sei erforderlich; falls er sich weigere, würde er die Polizei rufen.

Das Bundesdatenschutzgesetz lässt das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zu, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.[116] Die DB AG hat ein berechtigtes (wirtschaftliches) Interesse daran, den ihr zustehenden erhöhten Fahrpreis einzufordern. Zweck der Datenerhebung ist einerseits die Beitreibung des erhöhten Beförderungsentgelts und zum anderen die Erfassung von Wiederholungsfällen. Hat der Fahrgast keinen Personalausweis bei sich, müssen Name und Anschrift über ein anderes Dokument nachgewiesen werden. Allerdings enthält weder der Pass noch der Aufenthaltstitel eine Anschrift des Betroffenen. Insoweit war die Datenerhebung bezüglich des Aufenthaltstitels nicht erforderlich und damit unzulässig.

Aufgrund unserer Intervention verzichtet die DB AG nunmehr bei der Ausstellung von Fahrpreisnacherhebungen auf die Erhebung von Aufenthaltstiteln (wie Aufenthaltsgenehmigung, Aufenthaltserlaubnis oder Duldung) auf den mobilen Terminals. Zur Bestimmung der Adresse wird die kontrollierende Person künftig den Fahrgast um die freiwillige Vorlage einer Meldebescheinigung, eines anderen amtlichen Dokuments oder einer sonstigen geeigneten Unterlage (z. B. adressierten Briefs einer Behörde oder Institution) bitten. Nur wenn solche Dokumente nicht vorgelegt werden, wird eine Personalienfeststellung durch die Bundes- und Landespolizei vorgenommen.

116 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Die Erfassung des Aufenthaltstitels durch die DB AG im Rahmen von Fahrpreisnacherhebungen ist zur Verfolgung ihrer Geschäftsinteressen nicht erforderlich und damit unzulässig.

5.3 Ein zu lange wirkender Führerscheinentzug

Aus der Praxis

Ein Bürger, dem die Fahrerlaubnis nach deren Entzug wiedererteilt worden war, bat das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) um eine Bescheinigung darüber, dass er schon zuvor eine Fahrerlaubnis besessen hatte. Einen solchen Nachweis benötige er für die Arbeitssuche und um einen Mietwagen zu bekommen. Die daraufhin erteilte Bescheinigung enthielt neben dem kürzlich vollzogenen Fahrerlaubnisentzug einen weiteren, der mehr als 30 Jahre zurücklag.

Wir wiesen das LABO auf die Fristen hin, nach denen Eintragungen im Verkehrszentralregister (VZR) getilgt werden[117]. Es bestand schließlich Einigkeit, dass der erste Fahrerlaubnisentzug im VZR nicht mehr gespeichert sein und dass die Tat und die Entscheidung nicht mehr zum Nachteil des Betroffenen verwertet werden durften[118]. Das LABO ist unserer Empfehlung gefolgt und hat eine neue Bescheinigung ausgestellt, die die Vorbesitzzeiten der Fahrerlaubnis positiv aufführt. Zusätzlich konnte der Hinweis aufgenommen werden, dass über frühere Zeiten des Fahrerlaubnisbesitzes nach Maßgabe der einschlägigen Tilgungsbestimmungen keine Angaben gemacht werden können. Auf Wunsch des Antragstellers konnte auf diesen Hinweis verzichtet werden.

Darüber hinaus vertrat das LABO die Ansicht, dass aufgrund der Pflicht zur Aktenführung und zur vollständigen Dokumentation des Geschehensablaufs nicht alle Unterlagen aus den Führerscheinakten entfernt werden müssen. So könne z. B. die Verfügung über den Fahrerlaubnisentzug in der Akte verbleiben. Die Unterlagen dürften lediglich nicht mehr zum Nachteil der oder des Betroffenen verwertet werden.

117 § 29 StVG
118 § 29 Abs. 8 StVG

Ob es sich hier um einen Einzelfall handelt oder sich erneut die jahrelang geführte (und beendet geglaubte) Grundsatzdiskussion[119] um die fristgerechte Bereinigung der Führerscheinakten auftut, bleibt zu überprüfen.

Nachweise über Vorbesitzzeiten von Fahrerlaubnissen sollten keine Angaben zu Entzugszeiten beinhalten, die im Verkehrszentralregister bereits gelöscht wurden.

119 Vgl. JB 2000, 4.2.3.; JB 2003, 4.2.2 (a. E.)

6. Justiz

6.1 Offenbarung von Opferdaten bei DNA-Reihenuntersuchung

Aus der Praxis

Die Staatsanwaltschaft leitete 2008 ein Ermittlungsverfahren gegen unbekannt wegen des Verdachts der Vergewaltigung und des schweren sexuellen Missbrauchs von Kindern ein. Nachdem umfangreiche Ermittlungen nicht zur Feststellung des Täters führten, ordnete das Amtsgericht Tiergarten die Durchführung einer DNA-Reihenuntersuchung an, die wir überprüften.

Bei Durchsicht der Ermittlungsakten stellten wir fest, dass die zu testenden Personen aufgrund des Gerichtsbeschlusses Kenntnis von Vor- und Nachnamen der Opfer nehmen konnten, weil die Staatsanwaltschaft diese Daten vor Übersendung der gerichtlichen Entscheidung nicht anonymisiert hatte.

Die Übermittlung personenbezogener Opferdaten an potenzielle Täter ist ohne Einwilligung der Geschädigten unzulässig. Die Offenbarung der Identität der Opfer ist für die Begründung der gerichtlichen Anordnung ebenso wenig erforderlich wie für die Belehrung der zu testenden Personen über die Freiwilligkeit der Entnahme einer DNA-Probe und die damit einhergehende Aufklärung über den Verwendungszweck der entnommenen Körperzellen.

Zwar kann die Staatsanwaltschaft personenbezogene Daten in richterlichen Beschlüssen grundsätzlich nicht ohne Beteiligung des Gerichts anonymisieren. Jedoch hat die Staatsanwaltschaft aufgrund eigener Schutzobliegenheiten gegenüber den Prozessbeteiligten die Pflicht, eigenverantwortlich zu prüfen, ob die Gefahr der unzulässigen Datenübermittlung an Dritte besteht.

Die Staatsanwaltschaft sollte daher im Vorfeld einer gerichtlichen Anordnung darauf hinwirken, dass eine solche Entscheidung nur personenbezogene Daten enthält, deren Angabe den Schutz von Prozessbeteiligten, Zeugen und Geschädigten nicht gefährdet. Darüber hinaus ist die Staatsanwaltschaft auch nach Erlass eines Gerichtsbeschlusses, für dessen Zustellung sie zuständig ist, verpflichtet zu überprüfen, ob der Entscheidungsinhalt den Schutz der vorgenannten Personen gewährleistet. Gegebenenfalls hat die Staatsanwaltschaft bei dem zuständigen Gericht vor Zustellung einer solchen Entscheidung auf eine Abänderung des Beschlusses hinzuwirken.

Der Generalstaatsanwalt teilte uns im Zusammenhang mit dem Erlass einer weiteren Gerichtsentscheidung zur Durchführung einer DNA-Reihenuntersuchung in diesem Ermittlungsverfahren mit, dass die Polizei zur Gewährleistung des Datenschutzes den zu testenden Personen nunmehr eine auszugsweise Ausfertigung des Beschlusses aushändigt, in dem nur die Anfangsbuchstaben der Nachnamen der Geschädigten erscheinen.

Es ist sicherzustellen, dass im Rahmen der DNA-Reihenuntersuchung keine personenbezogenen Daten der Opfer an potenzielle Täter übermittelt werden.

6.2 Kontrollbefugnis der Aufsichtsbehörde gegenüber Rechtsanwälten

Bereits 2005 haben wir darauf hingewiesen, dass für Rechtsanwälte das Bundesdatenschutzgesetz (BDSG) gilt und sie der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterliegen[120]. Die Berliner Rechtsanwaltskammer sowie die Bundesrechtsanwaltskammer waren dagegen der Auffassung, die Bundesrechtsanwaltsordnung (BRAO) regele die Pflichten zum Umgang mit mandatsbezogenen Daten abschließend. Unsere Rechtsansicht wurde nunmehr durch einen Beschluss des Kammergerichts[121] im Grundsatz bestätigt.

Diese Entscheidung beendete einen Rechtsstreit wegen eines Bußgeldbescheids, den wir 2006 gegen einen Rechtsanwalt erlassen hatten, der uns unter Berufung auf seine anwaltliche Verschwiegenheitspflicht keine Auskunft erteilte. Das Kammergericht entschied, dass die BRAO die anwaltlichen Pflichten im Umgang mit Daten, die Kontroll- und Aufsichtspflichten sowie die Sanktions-

120 JB 2005, 4.3
121 Vom 20. August 2010, 1 Ws (B) 51/07 – 2 Ss 23/07

möglichkeiten nur rudimentär bestimmt und keinen mit dem Schutzzweck des BDSG vollständig übereinstimmenden Regelungsgehalt hat, weshalb das **BDSG anwendbar** bleibt.

Dennoch sah das Gericht im vorliegenden Fall die festgestellte Auskunftsverweigerung des Rechtsanwalts nicht als eine Ordnungswidrigkeit an, weil dieser einer gesetzlichen Verschwiegenheitspflicht[122] unterlag, bei dessen Nichtbeachtung er der Gefahr einer strafrechtlichen Verfolgung ausgesetzt gewesen wäre.

Berufen sich Rechtsanwälte gegenüber der Aufsichtsbehörde nicht auf die Gefahr einer strafgerichtlichen Verfolgung oder besteht diese nicht, ist die Aufsichtsbehörde weiterhin befugt, die Einhaltung datenschutzrechtlicher Vorschriften durch Rechtsanwälte zu kontrollieren und Verstöße zu ahnden.

6.3 Anwaltsnotare im Grundbuchamt

Wir erhielten zwei Beschwerden darüber, dass Rechtsanwälte, die gleichzeitig als Notare tätig sind, zu anwaltlichen Zwecken Auszüge aus dem Grundbuch bei dem Grundbuchamt anforderten oder aus dem elektronisch geführten Grundbuch abfragten, ohne hierfür ein berechtigtes Interesse darzulegen.

Gesetzlich ist es jedem gestattet, Einsicht in das Grundbuch zu nehmen, der ein berechtigtes Interesse dargelegt hat[123]. Notare sind von dieser Darlegungspflicht aufgrund ihrer herausgehobenen Stellung als Träger eines öffentlichen Amtes befreit. Rechtsanwälte müssen jedoch ebenso wie andere private Stellen ein berechtigtes Interesse darlegen, damit gewährleistet werden kann, dass Unbefugte keinen Einblick in die Rechts- und Vermögensverhältnisse der im Grundbuch eingetragenen Personen erhalten.

122 § 203 Abs. 1 Nr. 3 StGB
123 § 12 Abs. 1 Satz 1 GBO

Rechtsanwälte, die gleichzeitig Notare sind, sind gesetzlich verpflichtet, die **Ausübung dieser Funktionen strikt zu trennen.** Ein Anwaltsnotar muss bei seiner Tätigkeit klar zum Ausdruck bringen, ob er gerade als Rechtsanwalt oder als Notar tätig ist. Es ist unzulässig, als Notar einen Grundbuchauszug anzufordern, um diesen anwaltlich zu nutzen. Auch ein zunächst für notarielle Zwecke angeforderter Grundbuchauszug darf später nicht für anwaltliche Zwecke verwendet werden. Das tatsächliche Bestehen eines berechtigten Interesses an dem Datenabruf entbindet einen Rechtsanwalt ebenfalls nicht von seiner gesetzlichen Pflicht, dies beim Datenabruf darzulegen. Wir haben die beiden Rechtsanwälte aufgefordert, dies künftig zu beachten.

Anwaltsnotare müssen, wenn sie „nur" anwaltlich tätig sind, bei Anträgen auf Grundbucheinsicht das berechtigte Interesse darlegen.

6.4 Unbegrenzte Einsicht in Strafverfahrensakten bei der Bewerberauswahl?

Ein Petent beschwerte sich darüber, dass eine Berliner Hochschule, bei der er sich als wissenschaftlicher Mitarbeiter beworben hatte, Einblick in die Akte eines gegen ihn geführten Strafverfahrens bekommen hatte. Das Strafverfahren war aufgrund einer Anzeige der Hochschule eingeleitet worden, weil diese den Verdacht hegte, der Petent habe sich mit gefälschten Zeugnissen beworben.

Die Hochschule hatte im Strafverfahren „als Geschädigte" die Übersendung der Strafakte beantragt, ohne dies näher zu begründen. Daraufhin übersandte das Amtsgericht Tiergarten die gesamte Akte, die auch einen Vermerk zu einer Hausdurchsuchung bei dem Petenten enthielt. Diesem war zu entnehmen, dass die Wohnung des Petenten völlig verdreckt sei, dass er Depressionen habe und von Hartz-IV-Leistungen lebe. Die Hochschule erklärte im Nachhinein, die Übersendung der Strafakte sei zur Abwehr von Schadensersatzansprüchen im Zusammenhang mit der mutmaßlichen Straftat erforderlich gewesen.

Die Übersendung der gesamten Akte war rechtswidrig. Öffentlichen Stellen wie einer Hochschule können Strafverfahrensakten zur Einsicht nur übersandt werden, soweit dies zur Feststellung, Durchsetzung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist, und wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern würde oder die Akteneinsicht begehrende Stelle unter Angaben von Gründen erklärt, dass die Erteilung einer Auskunft zur Erfüllung ihrer Aufgabe nicht ausreichen würde[124]. Diese Voraussetzungen lagen hier nicht vor. Weder hat die Hochschule ihren Antrag auf Aktenübersendung begründet, noch ist ersichtlich, dass die Erteilung von Auskünften aus der Akte einen unverhältnismäßigen Aufwand erfordert hätte oder die Kenntnis der gesamten Akte zur Abwehr von Schadensersatzansprüchen erforderlich war. Wir haben daher einen Mangel festgestellt und das Amtsgericht Tiergarten zu einem datenschutzkonformen Vorgehen in der Zukunft aufgefordert.

Gerichte müssen sicherstellen, dass Akteneinsichtsanträge öffentlicher Stellen für verfahrensübergreifende Zwecke zur Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen entsprechend den gesetzlichen Vorgaben geprüft werden.

124 § 474 Abs. 2 Satz 1 Nr. 1, Abs. 3, Abs. 5 StPO

7. Finanzen

7.1 Kirchensteuer

7.1.1 Bundesweite Datenbank zur Religionszugehörigkeit?

Mit dem Unternehmenssteuerreformgesetz 2008 hat der Gesetzgeber in den §§ 43 ff., 32 d Einkommensteuergesetz (EStG) eine Abgeltungssteuer auf Kapitalerträge eingeführt. Kapitalerträge, die nicht in einem Unternehmen anfallen, werden danach mit einem einheitlichen Steuersatz von 25 Prozent besteuert. Der Steuerabzug erfolgt direkt an der Quelle der Einkünfte (z. B. Geldinstitute, Banken) und wird von dort an die Finanzverwaltung abgeführt. Der Steuerpflichtige muss die Kapitalerträge grundsätzlich nicht mehr zusätzlich in seiner Einkommensteuererklärung angeben. Das Abzugssystem umfasst dabei auch die Kirchensteuer.

In einer Evaluierungsphase bis Ende Juni hatte der Bundesgesetzgeber den Steuerpflichtigen die Freiheit eingeräumt, selbst zu entscheiden, ob sie ihrer Bank durch Mitteilung ihrer Religionszugehörigkeit die Einbehaltung der Kirchenkapitalertragsteuer im Rahmen des Abgeltungssteuerverfahrens ermöglichen oder ob die Einbehaltung der Kirchenkapitalertragsteuer (wie bisher) im Rahmen der Veranlagung zur Einkommensteuer erfolgen soll[125]. Nach Abschluss der Evaluierungsphase sollten die Auswirkungen dieser **Wahlfreiheit der Steuerpflichtigen** auf das Vorhaben, für die Feststellung der Religionszugehörigkeit ein elektronisches Informationssystems beim Bundeszentralamt für Steuern einzurichten, in einem Bericht an den Bundestag dargelegt werden. Zur Einführung des § 51 a Abs. 2 e EStG heißt es in der Begründung zum Gesetzentwurf des Unternehmenssteuerreformgesetzes 2008[126]:

„*Ziel der Reform der Besteuerung von Kapitalerträgen ist es, auch bei der Erhebung der auf die Kapitalerträge anfallenden Kirchensteuer den Steuerabzug grundsätzlich an der*

125 § 51 a Abs. 2 c und d EStG
126 BT-Drs. 16/4841, S. 69 ff.

Quelle vorzunehmen. Dieses Ziel lässt sich nur erreichen, wenn die zum Abzug verpflichtete Stelle in Zukunft in die Lage versetzt werden kann, den Abzug entsprechend der Zugehörigkeit zu einer Religionsgemeinschaft auf einfache Weise durchzuführen oder zu unterlassen, falls keine entsprechende Mitgliedschaft vorliegt. Dies wird mit der Einrichtung einer Datenbank ermöglicht, die es den Stellen, die die Kapitalertragsteuer einzubehalten haben, erlaubt, auf elektronischem Wege festzustellen, ob ein Steuerpflichtiger Angehöriger einer Religionsgemeinschaft ist oder nicht, und gegebenenfalls, welcher Religionsgemeinschaft er angehört und welcher Kirchensteuersatz für ihn anzuwenden ist. […] Eine derartige Datenbank wird allerdings voraussichtlich nicht vor dem Veranlagungszeitraum 2011 zur Verfügung stehen […]. Sobald die Überprüfung ergibt, dass beim Bundeszentralamt für Steuern die Daten über die Religionszugehörigkeit der Steuerpflichtigen verfügbar sind, wird durch ein weiteres Gesetzgebungsverfahren ein zwingendes Quellensteuerabzugssystem mit der Möglichkeit einer elektronischen Abfrage des Religionsmerkmales beim Bundeszentralamt eingeführt. Die Bundesregierung wird daher die Wirksamkeit der Vorschriften überprüfen, um ein entsprechendes Gesetzgebungsverfahren einzuleiten. Damit wird es auch möglich, die zu findende Lösung an die neuesten technischen Entwicklungen anzupassen. Das bis zur Einführung dieses Systems vorgesehene, dem Kirchensteuerpflichtigen eingeräumte Wahlrecht (Einbehalt der Kirchensteuer im Abzugsverfahren oder Veranlagung durch das zuständige Finanzamt) stellt sich vor diesem Hintergrund als eine Übergangslösung für einen begrenzten Zeitraum dar."

Da es sich bei den Angaben zur Religionszugehörigkeit um sensitive Daten handelt, hatten sich die Datenschutzbeauftragten bereits im Gesetzgebungsverfahren zum Unternehmenssteuerreformgesetz 2008 dafür eingesetzt, dass den Banken dieses Datum im Abzugsverfahren der Abgeltungssteuer nicht mitgeteilt werden darf. Die grundsätzlichen Bedenken gegenüber dem Verfahren stellten die Datenschutzbeauftragten angesichts des Wahlrechts, das den Steuerpflichtigen für die Evaluierungsphase eingeräumt wurde, zurück. In der Erwartung einer ergebnisoffenen Evaluierung mussten die Datenschutzbeauftragten feststellen, dass der erste Entwurf des vom Bundesministerium der Finanzen (BMF) vorgelegten Evaluierungsberichts **keine substanziierte Prüfung der datenschutzrechtlichen Fragen** und Probleme enthielt. In intensiven Gesprächen konnte erreicht werden, dass die datenschutzrechtlichen Belange im abschließenden Bericht[127] Berücksichtigung fanden. Insbesondere wurde ein von den Datenschutzbeauftragten entwickeltes (alternatives) Modell in den

127 BT-Drs. 17/2865

Bericht aufgenommen, das den Abzug der Kirchensteuer an der Quelle ermöglicht, ohne dass die Kirchensteuerabzugsverpflichteten (z. B. die Bank) Kenntnis von der Religionszugehörigkeit der Steuerpflichtigen erhält[128].

Der Bericht der Bundesregierung zur Evaluierung des Kirchensteuerabzugsverfahrens zeigt alternative datenschutzfreundliche Modelle der Datenerhebung auf. Er verweist diesbezüglich auf eine erforderliche Prüfung, die bislang noch nicht erfolgt ist.

7.1.2 Überprüfung der Religionszugehörigkeit durch Kirchensteuerstellen

Regelmäßig erreichen uns Beschwerden über die Zusendung eines Fragebogens zur „Feststellung der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft" durch die Finanzämter (Kirchensteuerstelle).

Nach dem Gesetz über die Erhebung von Steuern durch öffentlich-rechtliche Religionsgemeinschaften im Land Berlin[129] können Kirchen und andere Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, Steuern aufgrund eigener Steuerordnungen erheben. Zu diesem Zweck haben die Katholische und Evangelische Kirche gemeinsame Kirchensteuerstellen eingerichtet, die zwar eng mit den staatlichen Finanzämtern zusammenarbeiten und räumlich an diese angegliedert sind, rechtlich und organisatorisch jedoch zu den Kirchen gehören.

Während die Finanzämter die Berechnung der Kirchensteuer zusammen mit der Berechnung der übrigen Steuern durchführen, überprüfen die Kirchensteuerstellen lediglich den Umstand, ob jemand aufgrund der Zugehörigkeit zu einer Religionsgemeinschaft kirchensteuerpflichtig ist. Eine Überprüfung

128 Näheres dazu: BT-Drs. 17/2865 (C. IV.2.)
129 KiStG vom 4. Februar 2009, GVBl. S. 23

ist dann notwendig, wenn ein Finanzamt von sich aus nicht ohne Weiteres feststellen kann, ob eine Kirchenzugehörigkeit vorliegt oder nicht.

Das Recht der Kirchensteuerstellen zur Überprüfung der Religionszugehörigkeit ergibt sich aus Art. 140 Grundgesetz (GG) in Verbindung mit Art. 136 Abs. 6 und 8 Weimarer Reichsverfassung. Diese Bestimmung der Weimarer Reichsverfassung ist aufgrund der Verweisung in Art. 140 GG Bestandteil des Grundgesetzes. Grundsätzlich ist danach niemand verpflichtet, seine religiöse Überzeugung zu offenbaren. Jedoch heißt es in Art. 136 Abs. 3 Satz 2 Weimarer Reichsverfassung:

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

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

Die Kirchensteuerstellen erhalten von den Finanzämtern an personenbezogenen Daten Steuernummer, Religionsmerkmal, Namen, Vornamen, Geburtsdatum, Anschrift sowie die Angabe, ab wann das Steuerkonto aufgenommen wurde. In der Regel wird sich anhand dieser Angaben die rechtliche Zugehörigkeit oder Nichtzugehörigkeit zur Evangelischen oder Katholischen Kirche feststellen lassen. Eine weitergehende Prüfung der Religionszugehörigkeit erfolgt nur in den Fällen, in denen Abweichungen zwischen vorliegender Grundinformation, Lohnsteuerkarte oder Angaben in der Steuererklärung auftreten. Der Fragebogen wird nur versandt, wenn die Zugehörigkeit zu einer Kirche nicht bereits eindeutig geklärt werden konnte. Hierbei ist problematisch, dass den Kirchensteuerstellen auch bei an sich eindeutigen Fällen die notwendigen Informationen nicht zur Verfügung stehen. Dies liegt zum Teil in dem fehlenden Abgleich zwischen kirchlichen Stellen und den Finanzämtern begründet[130], zum Teil in dem innerkirchlichen Organisationsaufbau. So werden

130 Z. B. geben Steuerpflichtige nach einem Umzug gegenüber der Meldebehörde ihre Kirchenzugehörigkeit nicht an, obwohl sie tatsächlich nicht aus der Kirche ausgetreten sind.

die Daten über Kirchenmitglieder in der Gemeinde der Taufe geführt, nicht in der des Wohnsitzes. Die Kirchensteuerstellen haben danach nur die Möglichkeit, die Angaben durch den Fragebogen bei den Steuerpflichtigen selbst zu erheben.

Aufgrund des verfassungsmäßig garantierten Selbstverwaltungsrechts der Kirchen (Art. 137 Abs. 3 Weimarer Reichsverfassung i. V. m. Art. 140 GG) ist es dem Staat verwehrt, die Kirchen über den Umweg der Datenverarbeitung beim Einzug der Kirchensteuer zu beaufsichtigen. Die Einhaltung des Datenschutzes in diesem Bereich wird daher von eigenständigen Datenschutzaufsichtsinstanzen der Religionsgemeinschaften wahrgenommen.

7.2 Wenn die Daten nicht umgehend fließen ...

Eine Bürgerin wurde mit ihrem Kraftfahrzeug abends von der Polizei angehalten und zur Kontrolle auf einen Parkplatz geleitet. Zur Begründung wurde angegeben, dass die Kraftfahrzeugsteuer für den Pkw nicht bezahlt worden sei. Obwohl die Bürgerin dies bestritt, hinderten die Polizeibeamten sie an der Weiterfahrt, „entstempelten" das Kraftfahrzeug und brachten einen gelben Aufkleber an mit dem Zusatz „Fehlende Steuer". Was war hier geschehen?

Das Finanzamt Pankow/Weißensee hatte beim Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) beantragt, das Fahrzeug wegen nicht entrichteter Kraftfahrzeugsteuer außer Betrieb zu setzen. Da der Halter (wegen einer zwischenzeitlich geänderten Meldeanschrift) nicht auf die Aufforderung des LABO reagierte, entweder die fällige Steuer zu entrichten oder das Fahrzeug außer Betrieb zu setzen, wurde der zuständige Polizeiabschnitt mit der zwangsweisen Stilllegung des Fahrzeuges beauftragt. Da auch diese Maßnahme erfolglos blieb, wurde das Fahrzeug zur Fahndung ausgeschrieben. Nachdem der Kfz-Halter unter seiner neuen Meldeanschrift erneut angeschrieben und über die eingeleiteten Maßnahmen informiert worden war, bezahlte er die Kfz-Steuer einschließlich der Säumniszuschläge beim nunmehr zuständigen Finanzamt Prenzlauer Berg. Allerdings wurde das LABO vom Finanzamt über diesen Umstand nicht informiert. Dies hatte zur Folge, dass das Fahrzeug – trotz

bezahlter Steuerschuld – weiterhin zur Fahndung ausgeschrieben war. Mehr als fünf Monate später geriet die Bürgerin mit dem Fahrzeug in die abendliche Polizeikontrolle. Die polizeiliche Überprüfung des amtlichen Kennzeichens ergab – wie nicht anders zu erwarten –, dass das Fahrzeug aufgrund nicht gezahlter Kraftfahrzeugsteuer zur Fahndung ausgeschrieben ist. Eine telefonische Nachfrage beim Finanzamt oder beim LABO durch die Polizeibeamten vor Ort war nicht möglich, da diese Stellen zum Zeitpunkt der Kontrolle (um 21:30 Uhr) nicht mehr besetzt waren. Daraufhin wurde die Bürgerin an der Weiterfahrt mit dem (vermeintlich unversteuerten) Fahrzeug von den Polizeibeamten gehindert und das Fahrzeug „entstempelt". Dabei wurde ein gelber Punkt auf der Windschutzscheibe des Fahrzeugs angebracht mit Angaben zum Tag des Anbringens, zum amtlichen Kennzeichen und Abstellort sowie dem handschriftlichen Hinweis „Fehlende Steuer".

Die Übermittlung der Daten über die rückständige Kraftfahrzeugsteuer des Fahrzeughalters und die Einleitung des Verfahrens zur Zwangsentstempelung war datenschutzrechtlich zulässig[131]. Die Zulassungsstelle hat, wenn die Kraftfahrzeugsteuer nicht entrichtet worden ist, auf Antrag der für die Kraftfahrzeugsteuer zuständigen Stelle das Kfz von Amts wegen abzumelden. Da der Halter des Fahrzeuges zunächst nicht auf die Aufforderung des LABO reagierte, entweder das Fahrzeug außer Betrieb zu setzen oder die Entrichtung der Steuer nachzuweisen, wurde das Fahrzeug vom LABO rechtmäßig zur Fahndung ausgeschrieben.

Allerdings sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten während der Verarbeitung korrekt, vollständig und aktuell bleiben **(Datenintegrität)**[132]. Dem entspricht die Regelung über „rückstandsunterbindende Maßnahmen" zu „4. Zahlung der Kraftfahrzeugsteuer" in der Vollstreckungskartei der Finanzverwaltung. Danach hat die Finanzbehörde die Zulassungsstelle unverzüglich darüber in Kenntnis zu setzen, wenn der Schuldner die rückständige Kraftfahrzeugsteuer entrichtet hat. Dem Schuldner ist eine Bescheinigung zur Vorlage bei der Zulassungsstelle zu erteilen, dass keine Rückstände mehr bestehen. Vorliegend ist die zeitnahe Meldung über die vollständige Tilgung der Steuerschulden durch das Finanzamt an das LABO

131 § 14 Abs. 1 KraftStG
132 § 5 Abs. 2 Nr. 2 BlnDSG

unterblieben. Infolgedessen war der im LABO geführte Datenbestand zum Zeitpunkt der Polizeikontrolle nicht mehr aktuell. Es lag ein Verstoß gegen § 5 Abs. 2 Nr. 2 BlnDSG vor.

Mit dem handschriftlichen Zusatz „Fehlende Steuer", den die Polizeimitarbeiter auf dem gelben Aufkleber am Fahrzeug vermerkten, wurden darüber hinaus personenbezogene Daten der Bürgerin gegenüber der Öffentlichkeit offenbart, rechtlich also an Dritte übermittelt. Eine Rechtsgrundlage für eine solche Datenübermittlung mit **„Prangerwirkung"** ist selbst dann nicht ersichtlich, wenn der Steuerrückstand nicht beglichen worden wäre. Der Polizeipräsident hat eingeräumt, dass auch die entsprechende interne Geschäftsanweisung einen derartigen Hinweis nicht vorsieht.

Wer Datenübermittlungspflichten hat, muss diesen umgehend nachkommen. Anderenfalls führt das zu inaktuellen Datenbeständen bei den vorgesehenen Empfängern, die dann zulasten der Betroffenen gehen können. Werden Fahrzeuge von der Polizei stillgelegt, so darf dies nicht mit einer öffentlichen Bloßstellung durch Angabe der Gründe verbunden werden.

8. Sozialordnung

8.1 Sozial- und Jugendverwaltung

8.1.1 Wenn das Jobcenter die Klassenfahrt bezahlt

Aus der Praxis

Die Mutter einer Schülerin, die an einer von der Schule ausgerichteten Kursfahrt teilnehmen wollte, wurde vom Jobcenter aufgefordert, den für die Kostenübernahme verwendeten Antrag von der Schule ausfüllen und mit einem Schulstempel versehen zu lassen. Zudem bestand das Jobcenter darauf, den Zahlbetrag direkt auf das Konto der die Fahrt leitenden Lehrkraft zu überweisen.

Durch das vom Jobcenter vorgegebene Verfahren erfährt die Schule zwangsläufig vom Leistungsbezug der Mutter. Auf diese Weise wird das Recht der Mutter, selbst über die Preisgabe ihrer Sozialdaten zu entscheiden, eingeschränkt. Diese Entscheidungsfreiheit ist ein wichtiger Bestandteil des Grundrechts auf informationelle Selbstbestimmung. Auch besteht keine Notwendigkeit dafür, einen vorgegebenen Vordruck zu verwenden, soweit die Antragstellenden die erforderlichen Nachweise gegenüber dem Sozialleistungsträger anderweitig erbringen können.

Um das Recht der Antragstellenden auf informationelle Selbstbestimmung zu wahren, haben wir empfohlen, nicht nur den besagten Vordruck, sondern zusätzlich ein alternatives Antragstellungsverfahren anzubieten. Diese Alternative muss gewährleisten, dass die Schule nichts vom Leistungsbezug erfährt. Die Leistungsempfangenden müssen die Möglichkeit haben, die erforderlichen Nachweise auch ohne Verwendung des Vordrucks zu erbringen. Vor allem muss das Jobcenter auf diese Alternative und auf eine mit dieser ggf. einhergehenden Verzögerung der Antragsbearbeitung hinweisen. Diese Verzögerung darf nicht zu Lasten der Betroffenen gehen.

Darüber hinaus gilt im Sozialrecht die Regel, dass die gewährte Leistung direkt auf das Konto der Leistungsempfangenden überwiesen wird. Ein Argument dafür, warum hier von dieser Regel abgewichen werden und die Leistung auf

das Konto der Lehrkraft überwiesen werden soll, ist nicht zu erkennen. Insbesondere ist keine erhöhte Zweckentfremdungsgefahr erkennbar. Denn die Eltern der Schülerinnen und Schüler erhalten in der Regel bei Vorbereitung einer Klassenfahrt eine schriftliche Mitteilung über anfallende Kosten, eingegangene Zahlungen und mögliche Rückerstattungen. Eine Kopie davon können die Eltern beim Jobcenter einreichen. Kontrolle und Kostentransparenz wären somit in jedem Fall gegeben.

Das vom Jobcenter geforderte Verfahren basierte auf einer Vorgabe der Senatsverwaltung für Integration, Arbeit und Soziales. Nachdem wir ihr gegenüber einen datenschutzrechtlichen Mangel festgestellt hatten, hat sie sich unserer Rechtsauffassung angeschlossen. Zukünftig wird es zwei Varianten der Antragstellung geben, d. h., eine Verwendung des Vordrucks ist ebenso wenig zwingend wie eine Überweisung des Geldbetrages direkt vom Jobcenter auf das Konto der die Fahrt leitenden Lehrkraft. Die Form der Nachweiserbringung steht damit im Ermessen der Eltern. Vorgaben zum Inhalt der Nachweiserbringung bestehen lediglich insofern, als die Dauer und die Kosten der Fahrt, die Aufteilung der Kostenpositionen und die Beantragung und Gewährung von Zuschüssen oder anderen vorrangigen Hilfen nachgewiesen werden müssen. Wird der Vordruck nicht verwendet, muss auch ein Nachweis über die Überweisung des Geldbetrages und über die Teilnahme der Schülerin oder des Schülers an der Klassenfahrt erbracht werden sowie darüber, dass es sich um eine Fahrt nach schulrechtlichen Bestimmungen handelt.

Bei der Beantragung der Übernahme von Klassenfahrtkosten sind die Eltern in der Wahl der Mittel zur Erbringung der vom Jobcenter zur Antragsbearbeitung benötigten Nachweise frei. Auf diese Wahlfreiheit sind die Eltern vom Jobcenter hinzuweisen. Der Geldbetrag kann, je nach gewählter Verfahrensvariante, entweder vom Jobcenter oder von den Eltern selbst auf das Konto der verantwortlichen Lehrkraft überwiesen werden.

8.1.2 Sachverhaltsaufklärung und Datenerhebung durch die Betreuungsbehörde

Aufgrund einer Beratungsanfrage der Senatsverwaltung für Integration, Arbeit und Soziales haben wir uns mit der von Betreuungsbehörden zu leistenden Sachverhaltsaufklärung befasst.

Von Betreuung betroffen sind Erwachsene, die ihre Angelegenheiten aufgrund einer psychischen Krankheit oder einer Behinderung ganz oder teilweise nicht selbst regeln können. Im Betreuungsrecht geht es daher um die Frage, wie und in welchem Umfang für eine hilfsbedürftige Person vom Betreuungsgericht eine Betreuungsperson bestellt wird. Bei der vom Gericht zu leistenden Bewertung des Einzelfalls sowie bei der Gewinnung geeigneter Betreuungspersonen kommt die Betreuungsbehörde ins Spiel, in Berlin das zuständige Bezirksamt. Eine der gesetzlich festgelegten Aufgaben der Betreuungsbehörden ist, das Gericht zu unterstützen. Da das Betreuungsbehördengesetz selbst keine Befugnisse zur Datenverarbeitung enthält, ist das Berliner Datenschutzgesetz heranzuziehen[133]. Dieses verweist seinerseits auf das Bundesdatenschutzgesetz. Um eine unterstützende Leistung erbringen zu können, kann die Betreuungsbehörde die betroffene Person selbst befragen. Zu beachten ist dabei in jedem Fall, dass nur die für die Bearbeitung des jeweiligen Einzelfalls erforderlichen Daten erhoben werden. Diese müssen demnach unverzichtbar für die Aufgabenerfüllung der Betreuungsbehörde sein. Handelt es sich bei den benötigten Daten um besonders geschützte Daten, muss die Behörde vor der Datenerhebung zwingend die Einwilligung der betroffenen Person einholen. Zu den besonders geschützten Daten zählen beispielsweise Angaben über die körperliche oder psychische Gesundheit. Ist die betroffene Person aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, dürfen solche Daten in eng begrenzten Ausnahmefällen auch ohne ihre Einwilligung erhoben werden[134]. Liegen diese Voraussetzungen nicht vor, muss das Betreuungsgericht selbst die nötigen Ermittlungen durchführen.

Unter engen Voraussetzungen darf die Betreuungsbehörde die benötigten Daten auch bei anderen Personen als den Betroffenen erheben. Diese **Durchbrechung des sog. Direkterhebungsgrundsatzes** ist nur dann zulässig, wenn es sich nicht um besonders geschützte Daten handelt und die Erhebung bei der betroffenen Person nur mit einem unverhältnismäßigen Aufwand möglich wäre. Zudem muss stets die Frage gestellt werden, ob der Durchbrechung des Direkterhebungsgrundsatzes eventuell schutzwürdige Interessen der betroffenen Person entgegenstehen, die gegenüber den von der Betreuungsbehörde geltend gemachten Belange überwiegen.

Die Senatsverwaltung hat ein Rundschreiben für die örtlichen Betreuungsbehörden erlassen, in das diese Grundsätze aufgenommen wurden.

Will die Betreuungsbehörde das Betreuungsgericht bei dessen Tätigkeiten unterstützen, ist die Behörde grundsätzlich gehalten, die benötigten Daten bei der betroffenen Person zu erheben. Eine Sachverhaltsaufklärung ohne Mitwirkung der Betroffenen ist nur unter engen Voraussetzungen zulässig.

8.1.3 Übersendung von Jugendhilfeakten der DDR in Rehabilitierungsverfahren

Das Landgericht Berlin hat im Rahmen von Rehabilitierungsverfahren rechtsstaatswidrige strafrechtliche Maßnahmen oder andere Entscheidungen von Behörden über Freiheitsentzug in der ehemaligen DDR zu überprüfen. Grundlage hierfür ist das Strafrechtliche Rehabilitierungsgesetz (StrRehaG). Erweist sich die frühere Entscheidung als rechtsstaatswidrig bzw. willkürlich, sind die Betroffenen durch Gerichtsbeschluss zu rehabilitieren. Eine Aufhebung derartiger Entscheidungen begründet u. a. einen Anspruch der Betroffenen auf soziale Ausgleichsleistungen. Gegenstand des Rehabilitierungsverfahrens sind oftmals damalige Verfügungen über Heimeinweisungen. Um über die Rehabilitierungsanträge entscheiden zu können, benötigt das Landgericht die alten Jugendhilfeakten, Heimakten bzw. Jugendwerkhofakten aus den Archiven der Berliner Jugendämter.

Hier stellt sich die Frage, ob die Jugendämter auf Anforderung des Landgerichts die komplette Originalakte übersenden dürfen. Während die Betroffenen selbst

133 § 6 Abs. 2 BlnDSG
134 § 6 Abs. 2 BlnDSG i. V. m. § 13 Abs. 2 Nr. 3 BDSG

ihre Einwilligung in die Übersendung der Akten an das Landgericht erteilen, besteht oft das Problem, dass die Akten Daten Dritter enthalten, auf die sich die Einwilligung der Betroffenen nicht erstrecken kann. Die Daten der Dritten (z. B. Eltern, Lehrkräfte, Nachbarn) sind teilweise sensitiv, wenn es z. B. um die Darstellung familiärer Probleme oder Krankheiten geht. Für die Jugendämter stellt sich das Problem, dass es in der Praxis schwierig ist, Einwilligungserklärungen sämtlicher Dritter einzuholen.

Für die Weitergabe der Daten Dritter auch ohne deren Einwilligung enthält das Sozialgesetzbuch – Zehntes Buch (SGB X) eine ausreichende Rechtsgrundlage[135]. Die Übermittlung der personenbezogenen Daten aus Jugendhilfeakten der ehemaligen DDR an die Rehabilitierungskammer des Landgerichts erfolgt zu dem Zweck, diesem die Entscheidung über den Rehabilitierungsantrag nach dem StrRehaG zu ermöglichen und damit für das gerichtliche Verfahren. Die Übermittlung der Sozialdaten ist allerdings nur zulässig, wenn dies für die Entscheidung über die Rehabilitierung und die daran geknüpfte soziale Ausgleichsleistung erforderlich ist. Hierfür kann auch die Kenntnis der Daten Dritter erforderlich sein. Allerdings sind hier strenge Maßstäbe anzulegen. Es ist in jedem Einzelfall zu prüfen, ob die Daten tatsächlich notwendig sind. Auf etwaige schutzwürdige Interessen der Dritten ist bei der Prüfung ein besonderes Augenmerk zu richten, sodass nicht benötigte Daten zu schwärzen bzw. zu entfernen sind.

Dieses Verfahren stellt sicher, dass eine den Interessen der Opfer von rechtsstaatswidrigen Heimeinweisungen in der ehemaligen DDR gerecht werdende Übersendung der erforderlichen Informationen durch die Jugendämter an die Rehabilitierungskammer des Landgerichts erfolgt. Die Prüfung im Einzelfall gewährleistet, dass etwaige schutzwürdige Interessen Dritter nicht beeinträchtigt werden.

135 § 69 Abs. 1 Nr. 2 i. V. m. § 69 Abs. 1 Nr. 1 und § 69 Abs. 2 Nr. 1 SGB X

8.1.4 Der Zusammenhang von Kinderschutz und Datenschutz – ein nach wie vor wichtiges Anliegen

Maßnahmen und Konzepte zur Abwehr und Bekämpfung von Kindeswohlgefährdungen zu entwickeln, um damit in der Praxis einen effektiven Kinderschutz zu erreichen, ist seit Jahren für alle mit der Betreuung von Kindern und Jugendlichen betrauten Institutionen (wie öffentliche Jugendhilfe, freie Träger, Kinder- und Jugendgesundheitsdienste, Schulen) ein vordringliches Anliegen. Mit der Etablierung des Netzwerkes Kinderschutz auf der Senatsebene[136] wurde ein wichtiger Schritt in diese Richtung gemacht. Geht es um Maßnahmen zum Kinderschutz, ergeben sich immer wieder datenschutzrechtliche Fragen.

Die unzutreffende Aussage „Kinderschutz geht vor Datenschutz“ legt ein Spannungsverhältnis zwischen beiden Bereichen nahe. Auf der einen Seite wird (häufig aus Unkenntnis) immer wieder behauptet, die Datenschutzvorschriften würden die notwendige Kommunikation und Informationsweitergabe verhindern. Gleichzeitig wird die Forderung erhoben, die Datenschutzvorschriften deshalb zu ändern. Auf der anderen Seite begegnet uns zunehmend eine andere Sichtweise auf das Thema: Gerade diejenigen, die in ihrem Berufsalltag Kinder, Jugendliche und ihre Familien beraten und betreuen und für die der Aufbau eines Vertrauensverhältnisses zu den Familienmitgliedern eine selbstverständliche und unerlässliche Voraussetzung ihrer Arbeit ist, sind verunsichert, wenn von ihnen verlangt wird, mit anderen Institutionen zu „kooperieren“. Welche Möglichkeiten und Grenzen für derartige Kooperationen bestehen, war Gegenstand einer Vielzahl von Anfragen. Zum Thema „Datenschutz und Kinderschutz“ haben wir uns z. B. auf bezirklicher Ebene mit Vorträgen an den Kinderschutzkonferenzen der Jugendämter Tempelhof–Schöneberg und Treptow-Köpenick beteiligt. Die Stiftung SPI, Clearingstelle Jugendhilfe/Polizei, hat eine Veranstaltung zum Thema „Handlungssicherheiten im Kinderschutz und Datenschutz“ organisiert, in deren Rahmen wir einen Vortrag gehalten haben. Im November haben wir uns mit einem Vortrag „Kinderschutz und Datenschutz – (k)ein Widerspruch“ an einer gemeinsam von den Senatsverwaltungen für Gesundheit, Umwelt und Verbraucherschutz sowie für Bildung,

136 Vgl. JB 2006, 2.1

Wissenschaft und Forschung und der Charité Universitätsmedizin Berlin veranstalteten Fachtagung „Kinderschutz – Handeln im Rahmen interdisziplinärer Kooperation“ beteiligt.

Das Thema Kinderschutz war auch Gegenstand vieler Beratungsersuchen. Bereits Ende 2009 haben die Senatsverwaltungen für Gesundheit, Umwelt und Verbraucherschutz sowie für Bildung, Wissenschaft und Forschung und die LIGA der Wohlfahrtspflege in Berlin eine **„Rahmenvereinbarung zum Schutz von Kindern suchtkranker Eltern vor der Gefährdung des Kindeswohls“** geschlossen. Die Vereinbarung ist auf bezirklicher Ebene umzusetzen, was teilweise bereits geschehen ist. Hierbei soll die Kooperation aller Institutionen, die im jeweiligen Bezirk mit Familien mit Suchtproblemen Kontakt haben, verbindlich organisiert werden. Da Kooperationsvereinbarungen nicht geeignet sind, über die bestehenden Datenschutzgesetze hinausgehende Datenübermittlungsbefugnisse zu schaffen, haben wir deutlich gemacht, dass die gesetzlichen Datenschutzvorgaben zu beachten sind. Vor dem Hintergrund, dass in erster Linie Personen, die der beruflichen Schweigepflicht unterliegen, mit der Betreuung suchtkranker Personen betraut sind, bedarf es insofern im Einzelfall einer Einwilligung oder gesetzlichen Offenbarungsbefugnis, die sich z. B. aus dem Ende 2009 in Kraft getretenen Berliner Gesetz zum Schutz und Wohl des Kindes ergeben kann[137].

Die Senatsverwaltung für Bildung, Wissenschaft und Forschung hat einen **Handlungsleitfaden Kinderschutz für die Zusammenarbeit von Kindertageseinrichtungen und bezirklichem Gesundheitsamt und Jugendamt** herausgegeben. Er soll eine Hilfestellung für die Mitarbeiterinnen und Mitarbeiter im Umgang mit Kindeswohlgefährdungen geben und Verfahrensregelungen für die Zusammenarbeit der unterschiedlichen Institutionen schaffen. Da sich hier eine Reihe datenschutzrechtlicher Fragen stellt, insbesondere welche Datenübermittlungen zwischen den verschiedenen Einrichtungen zulässig sind, haben wir die mit der Erstellung des Leitfadens befasste Arbeitsgruppe ausführlich beraten. Unsere Anforderungen wurden aufgenommen.

137 § 11 Abs. 4 Berliner Kinderschutzgesetz; hierzu JB 2009, 7.1.2, S. 99 f.

Häufig wird ein falsch verstandener Datenschutz als Hindernis für eine notwendige Kooperation verschiedener Institutionen angeführt. Uns ist es wichtig, den Rahmen der zulässigen Kommunikation zwischen unterschiedlichen Stellen in Fällen von Kindeswohlgefährdung, aber auch deren Grenzen immer wieder aufzuzeigen. Datenschutzrechtliche Regelungen stehen einer im Einzelfall erforderlichen Kommunikation nicht entgegen. Ein staatlicher Schutz von Kindern kann jedoch nur gewährleistet werden, wenn Vertrauensverhältnisse zu betroffenen Familien geschützt und nicht hinter deren Rücken beliebig Informationen ausgetauscht werden.

8.1.5 Empfehlungen für den Umgang der Jugendämter mit Ersuchen von Strafverfolgungsbehörden

Nachdem wir auf Wunsch der Jobcenter Hinweise zum Umgang mit Anfragen der Polizei zu Sozialdaten von Leistungsempfangenden entwickelt hatten[138], haben wir entsprechende Empfehlungen zu den Anforderungen bei Datenübermittlungen an Polizeibehörden und die Amts- bzw. Staatsanwaltschaft auch für die Jugendämter entwickelt.

Anlass hierfür waren Hinweise aus der Praxis auf eine erhebliche Unsicherheit im Umgang mit derartigen Anfragen. Da der Bundesgesetzgeber eindeutige und abschließende Rechtsgrundlagen geschaffen hat, die die Übermittlung von Sozialdaten durch Sozialleistungsträger auf Ersuchen der Strafverfolgungsbehörden regeln, sahen wir uns veranlasst, diese Rechtslage in einer praxisgerechten Weise aufzubereiten und in Gestalt von Hinweisen den Jugendämtern zur Verfügung zu stellen. Praxisrelevant sind in erster Linie die §§ 68 und 73 Sozialgesetzbuch – Zehntes Buch (SGB X), die auch für die Jugendämter gelten[139]. § 68 SGB X enthält eine Übermittlungsbefugnis an die Strafverfolgungsbehörden. Die Daten sind explizit in der Vorschrift benannt. Es handelt sich um Namen, Vornamen, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen, derzeitigen oder zukünftigen Aufenthalt, Namen und Anschriften der derzeitigen Arbeitgeber. § 73 SGB X erlaubt die Übermittlung von Sozialdaten, soweit es zur Durchführung eines Strafverfahrens erforderlich ist.

138 JB 2009, 7.1.1
139 § 61 Abs. 1 Satz 1 SGB VIII

Es bedarf hierfür immer einer richterlichen Anordnung nach § 73 Abs. 3 SGB X. Soweit eine Übermittlung nicht zulässig ist, besteht keine Auskunftspflicht, keine Pflicht zur Vorlage oder Auslieferung von Schriftstücken, nicht automatisierten Dateien und automatisiert erhobenen, verarbeiteten oder genutzten Sozialdaten[140].

Eine wichtige Maßnahme beim Umgang mit Ersuchen von Strafverfolgungsbehörden ist die Benennung von verantwortlichen Beschäftigten, die über das jeweilige Ermittlungsersuchen zu entscheiden haben[141]. Die Strafverfolgungsbehörden sind ausschließlich an die benannte Mitarbeiterin bzw. den benannten Mitarbeiter zu verweisen. Die Jugendämter haben uns diese Verantwortlichen teilweise bereits konkret benannt.

Unsere Hinweise haben beim Polizeipräsidenten sowie der Senatsverwaltung für Inneres und Sport zu erheblichen Irritationen geführt. Dem liegt offenbar ein Missverständnis zugrunde. Die Empfehlungen beziehen sich ausschließlich auf Datenübermittlungen auf Ersuchen und damit auf einen sehr kleinen Ausschnitt der bei Datenübermittlungen zwischen Jugendämtern und Strafverfolgungsbehörden auftretenden Fragen. Fallkonstellationen, in denen das Jugendamt im Einzelfall zu dem Ergebnis gelangt, dass eine Übermittlung von Sozialdaten von Amts wegen an die Polizei zur Erfüllung gesetzlicher Aufgaben des Jugendamtes – nicht der Polizei – erforderlich ist, wie dies bei Vorliegen des Verdachts einer Kindeswohlgefährdung oder bei Kinder- und Jugenddelinquenz der Fall sein kann, sind nicht Gegenstand unserer Empfehlungen.

Zu begrüßen ist, dass mittlerweile im Rahmen der „Ressortübergreifenden Arbeitsgruppe Kinder- und Jugenddelinquenz“ unter der Federführung der Senatsverwaltung für Bildung, Wissenschaft und Forschung ein **Entwurf einer „Handreichung zur Datenübermittlung im Bereich Kinder- und Jugenddelinquenz“** erstellt worden ist, an dem wir maßgeblich mitgearbeitet haben.

140 § 35 Abs. 3 SGB I
141 § 68 Abs. 2 SGB X

Angesichts der in der Praxis bestehenden Unsicherheit im Umgang mit den Datenschutzvorschriften liegt uns daran, die Jugendämter in ihrer Arbeit dadurch zu unterstützen, dass ihnen die Bedeutung des Sozialgeheimnisses als eine wesentliche Voraussetzung für die Erfüllung ihrer Aufgaben verdeutlicht wird. Gleichzeitig ist es uns wichtig, den Beschäftigten eine Hilfestellung zu leisten, welche Befugnisse, aber auch Grenzen einer zulässigen Datenübermittlung gerade im Umgang mit Strafverfolgungsbehörden bestehen, und ihnen so mehr Rechtssicherheit zu geben.

8.2 Gesundheitswesen

8.2.1 Der Schutz von Patientendaten in Krankenhausinformationssystemen

Unsere Prüfungen haben gezeigt, dass in vielen Krankenhäusern die elektronischen Patientenakten einem zu weitem Kreis von Beschäftigten zugänglich sind. Wir wirken auf die Krankenhäuser ein, um sie zu einer Einschränkung dieser Zugriffsmöglichkeiten zu bewegen, und arbeiten in einer Arbeitsgruppe der Datenschutzkonferenz an der Etablierung von deutschlandweit geltenden Anforderungen an den Schutz von Patientendaten im Krankenhaus.

Jeder, der in einem Krankenhaus behandelt wird, hat ein Anrecht darauf, dass sich nur diejenigen durch Einblick in die Patientenakte über den Gesundheitszustand informieren können, die an der Behandlung und Pflege beteiligt sind. Wer die behandelnden Ärztinnen und Ärzte in der Diagnostik und Therapie unterstützt oder die Abrechnung der erbrachten Leistungen durchführt, darf in die Patientenakte Einblick nehmen, jedoch nur, soweit dies für die jeweilige Tätigkeit erforderlich ist.

Wie bereits berichtet[142], setzen einige Berliner Krankenhäuser ihrem Personal keine hinreichend engen Grenzen für den Zugriff auf Patientenakten. Es war und ist unser Ziel, diese Krankenhäuser dazu zu bewegen, die Grenzen so zu

142 JB 2009, 2.3

ziehen, dass die Zugriffsmöglichkeiten im Rahmen des Erforderlichen bleiben. Selbstverständlich muss diese Einschränkung in einer Weise erfolgen, dass die Arbeitsfähigkeit der Ärzteschaft und anderen Beschäftigten nicht behindert oder beschränkt wird.

Auf unsere Initiative begannen zwei Krankenhäuser mit besonders deutlichen Defiziten damit, Richtlinien zu erarbeiten, die den Bedarf an Zugriffen auf Patientenakten aus medizinischer Sicht mit klaren Grenzen umschreiben. Dies ist ein komplexes Unterfangen, da in einem modernen Krankenhaus die Behandlung hochgradig arbeitsteilig erfolgt. Es sind nicht nur die den verschiedensten Organisationseinheiten zugeordneten Ärztinnen und Ärzte, sondern auch viele Funktionskräfte vom Labor bis zum Sozialdienst zu berücksichtigen. Dennoch erwarten wir von den Krankenhäusern einen zügigen Abschluss der Erarbeitung von Richtlinien, welche die gesetzlichen Bestimmungen einhalten und die Erwartungen der Patientinnen und Patienten an die ärztliche Schweigepflicht und an einen für sie transparenten Umgang mit Daten über ihren Gesundheitszustand berücksichtigen.

Um für alle Berliner Krankenhäuser zu einheitlichen Vorgaben für den Umgang mit Patientenakten zu kommen, unabhängig davon, ob sie sich in öffentlicher, privater oder kirchlicher Hand befinden oder ob der Krankenhausträger in Berlin oder jenseits der Stadtgrenzen ansässig ist, setzten wir unsere Tätigkeit in der **Arbeitsgruppe zu Krankenhausinformationssystemen** fort, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im vergangenen Jahr unter unserer Federführung eingerichtet wurde.

Die Arbeitsgruppe erarbeitet eine **Orientierungshilfe**, die sich an Betreiber und Hersteller von Krankenhausinformationssystemen richtet. Diese Systeme bestehen aus einer Reihe von Komponenten. Jede davon muss derart gestaltet sein, dass sie ein datenschutzgerechtes Zusammenspiel im Gesamtsystem ermöglicht. Daher ist die Orientierungshilfe, die mittlerweile im Entwurf vorliegt, zweigeteilt: Der erste Teil konkretisiert die gesetzlichen Regeln. Der zweite besteht aus einem Anforderungskatalog für die Technik, die zum Führen der zentralen elektronischen Patientenakte in einem Krankenhaus angeboten und verwendet wird.

Krankenhauspersonal, das sich im eigenen Haus behandeln lässt, ist besonderen Risiken ausgesetzt. Auf unsere Initiative erprobt die Charité die Aufnahme von Beschäftigten als Patienten unter falschem Namen, wie dies in anderen Häusern bereits für Prominente praktiziert wird. Wir sind der Ansicht, dass diese Möglichkeit allen interessierten Beschäftigten offenstehen und bekannt sein muss. Auch dürfen ihnen aus der Wahrnehmung dieses Angebots keine zusätzlichen Bürden, etwa in der Abrechnung der für sie erbrachten Leistungen, erwachsen.

Krankenhäuser haben festzulegen, in welchem Maße der Zugriff auf Patientendaten für die Behandlung erforderlich ist, und über dieses Maß hinausgehende Zugriffe durch eine Kombination von organisatorischen Maßnahmen und technischen Mitteln zu unterbinden. Um eine unberechtigte Offenbarung feststellen und ahnden zu können, sind die Zugriffe zu protokollieren.

8.2.2 Mammographie-Screening

Aus Anlass mehrerer Beschwerden überprüften wir die Verarbeitung von Daten der Frauen, die von der Zentralen Stelle Mammographie-Screening zu Untersuchungen eingeladen wurden.

Zur Früherkennung von Brustkrebs wird in Berlin wie in den anderen Bundesländern für alle Frauen im Alter von 50 bis 70 Jahren die Teilnahme an regelmäßigen Untersuchungen angeboten, mit denen Brustkrebs im frühen Stadium erkannt werden soll. Die Frauen der jeweiligen Jahrgänge werden alle zwei Jahre eingeladen, an diesem Mammographie-Screening teilzunehmen. Die Einladung wird von einer zu diesem Zweck eingerichteten Zentralen Stelle ausgesprochen und ist mit dem Angebot eines konkreten Untersuchungstermins in einer hierfür spezialisierten Praxis verbunden. Hierzu erhält die Zentrale Stelle auf gesetzlicher Grundlage Meldedaten vom Landesamt für Bürger- und Ordnungsangelegenheiten.

Nicht alle angeschriebenen Frauen wünschen, an dem Screening-Programm teilzunehmen. Darüber hinaus ist für Frauen, bei denen Brustkrebs bereits diagnostiziert wurde oder die sich wegen dieser Krankheit behandeln lassen, die

Teilnahme an dem Screening nicht sinnvoll. Beide Gruppen von Frauen sind gebeten, sich bei der Zentralen Stelle telefonisch oder schriftlich zu melden, um von weiteren Einladungen für eine bestimmte Zeit oder endgültig ausgenommen zu werden.

Es bleibt daher nicht aus, dass die Mitarbeiterinnen der Zentralen Stelle sensitive Informationen über den Gesundheitszustand der Anruferinnen erhalten. Diese haben einen Anspruch darauf, dass nur der berechtigte Kreis von Personen Anrufe entgegennimmt und gesundheitliche Informationen nicht gespeichert werden. In der Tat genügt es für die Zentrale Stelle, lediglich den Zeitraum zu vermerken, innerhalb dessen keine weiteren Einladungen an die Anrufende gehen sollen. Der Grund hierfür spielt keine Rolle.

Dennoch hat die Zentrale Stelle regelmäßig Brustkrebsdiagnosen nicht nur erfasst, sondern es auch versäumt, die **technischen Sicherheitsvorkehrungen** zu treffen, die für die Verarbeitung von sensitiven Daten geboten sind. Eine unabhängige behördliche Datenschutzbeauftragte, die hierauf hätte dringen können, war nicht bestellt.

Des Weiteren haben nicht nur Mitarbeiterinnen der Zentralen Stelle für das Land Berlin, sondern auch solche der Zentralen Stelle Brandenburg Anrufe wechselseitig entgegengenommen, ohne dass hierfür eine gesetzliche Grundlage gegeben war und ohne dass dies für die betroffenen Frauen transparent wurde.

Wir haben erreicht, dass die Zentrale Stelle Berlin auf die Erfassung und Speicherung von Gesundheitsdaten verzichtet. Die beiden genannten Zentralen Stellen haben uns zugesagt, jeweils unter eigenem Namen zu operieren. Auf die Zusammenarbeit soll dennoch nicht verzichtet werden. Die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz und die brandenburgische Landesregierung sind aufgefordert, entweder die nötige gesetzliche Grundlage für diese Zusammenarbeit auf den Weg zu bringen oder im Zuge ihrer Aufsicht die Zusammenarbeit auf ein zulässiges, entweder vertraglich oder gesetzlich geregeltes Maß zu beschränken.

Auch ohne dass Gesundheitsdaten gespeichert werden, bedürfen die in der Zentralen Stelle verarbeiteten Daten des technischen Schutzes. Wir erwarten, dass die Zentrale Stelle im kommenden Jahr wie zugesagt den kleinen Schritten, die bereits erfolgt sind, einen systematischen Blick auf die **Informationssicherheit** folgen lässt und die erforderlichen Maßnahmen ergreift.

Die mit der Einladung der teilnahmeberechtigten Frauen beauftragte Zentrale Stelle ist nicht berechtigt, Daten über den Gesundheitszustand der angeschriebenen Frauen zu erfragen oder zu speichern. Die Zusammenarbeit mehrerer Zentraler Stellen bedarf gesetzlicher oder geeigneter vertraglicher Regelungen. Die verwendeten Meldedaten müssen in der Stelle und bei beauftragten Dritten angemessen gesichert werden.

8.2.3 Gemeinsames Krebsregister

Wir begleiteten die Behebung von Datensicherheitsmängeln, die wir im Vorjahr im Gemeinsamen Krebsregister (GKR) der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen feststellen mussten. Eine Reihe höchst unzulänglicher Sicherheitsvorkehrungen bleibt jedoch im Einsatz. Ersatz ist nicht geplant.

Das Gemeinsame Krebsregister (GKR) hat die Aufgabe, Daten über möglichst alle Diagnosen von Krebserkrankungen und auf solche Erkrankungen zurückführbare Todesfälle in den genannten Ländern zu registrieren, statistisch auszuwerten und der wissenschaftlichen Forschung für genehmigte Vorhaben zur Verfügung zu stellen. Es kann hierzu auf den größten Bestand an epidemiologischen Krebsregisterdaten der Bundesrepublik zurückgreifen. In Berlin sind Ärztinnen und Ärzte sowie Gesundheitsämter verpflichtet, die genannten Daten dem Krebsregister zu melden. Ärztinnen und Ärzte bedienen sich hierfür klinischer Tumorzentren, die die Daten regional sammeln und an das GKR weitergeben.

Wie bereits berichtet[143], wurden die Meldungen der Tumorzentren mit völlig unzureichendem Schutz per E-Mail an das GKR übermittelt. Da wir das

143 JB 2009, 7.2.2

GKR nicht davon überzeugen konnten, das Verfahren sofort einzustellen, sahen wir uns gezwungen, die Tumorzentren zu einer Einstellung der Übermittlungen aufzufordern. Erst nach dieser Einstellung der Sendungen stellte das GKR ein Alternativverfahren zur Verfügung. Die Meldungen erfolgen jetzt über verschlüsselte Datenträger. Die Erstellung dieser CD oder DVD darf nur auf besonders geschützten Geräten erfolgen.

Ein Einbruch in das Gemeinsame Krebsregister würde seinen gesamten (sensitiven) Datenbestand gefährden. Dem muss in zweierlei Hinsicht begegnet werden: Zum einen darf es Dieben nicht gelingen, sich Geräte und Datenträger des GKR anzueignen. Zum anderen müssen die Daten in einer Form gespeichert werden, dass Dritte sie nicht interpretieren und auf einzelne Personen beziehen können.

Um das erste Ziel zu erreichen, hat das GKR die defekte Einbruchsmeldeanlage instandsetzen und eine Verbindung zur Polizei schalten lassen, sodass auf einen Einbruch schnell reagiert werden kann.

Noch wichtiger ist es jedoch, das zweite Ziel zu erreichen, da damit auch Datendieben, welche über den Netzzugang des GKR in die dortigen Computer einzudringen suchen, der Zugriff wesentlich erschwert wird. Leider wurden vom GKR im Laufe des Jahres keinerlei Anstrengungen unternommen, ein angemessenes Niveau der Sicherheit seiner Informationstechnik zu erreichen. Die Vorarbeiten des Vorjahres blieben ungenutzt.

Die nur teilweise ausgeräumten jahrelangen Versäumnisse in der Durchsetzung des technischen Datenschutzes im Gemeinsamen Krebsregister erfordern entschlossenes Handeln des Krebsregisters und der für die Fachaufsicht zuständigen Senatsverwaltung für Gesundheit, Umweltschutz und Verbraucherschutz. Provisorien sind durch dauerhaft tragbare Verfahren zu ersetzen, die Planung der für die Datensicherheit im Register erforderlichen technischen Maßnahmen unverzüglich zu beginnen, und es ist für die Finanzierung und Umsetzung der Maßnahmen zu sorgen.

8.2.4 Tumorzentren

Der Nationale Krebsplan der Bundesregierung fordert einen flächendeckenden Ausbau der klinischen Krebsregister. Das war für uns Anlass, die Datenverarbeitung in den für die klinische Krebsregistrierung zuständigen Tumorzentren unter die Lupe zu nehmen.

Tumorzentren speichern Daten über die Erkrankung und Behandlung von Krebspatientinnen und -patienten. Ihr erklärtes Ziel ist die Auswertung der gesammelten Daten für die Sicherung der Qualität der Behandlung und für die Forschung über die Wirksamkeit von Krebstherapien. Außerdem sammeln sie Daten über Krebserkrankungen zur Übermittlung an das Gemeinsame Krebsregister[144]. Darüber hinaus übermitteln die Berliner Tumorzentren die Daten der Kranken, die hierin eingewilligt haben, auch an das Landestumorzentrum (Tumorzentrum Berlin e. V.) ebenfalls für Zwecke der Sicherung der Qualität der Krebsbehandlung in Berlin.

Wir haben das Tumorzentrum eines großen Krankenhauses daraufhin geprüft, ob die Daten ausschließlich für zulässige Zwecke verwendet und ausreichend geschützt werden.

Das Krankenhaus bildet für jeden Krebskranken eine **Tumordokumentation**, die von der Patientenakte getrennt elektronisch geführt wird. Treten Ärztinnen und Ärzte mehrerer Fachrichtungen in einer **Tumorkonferenz** zusammen, um die Behandlung einzelner Kranker zu diskutieren, so dienen Patientenakte wie Tumordokumentation als Datengrundlage. Die Patientinnen und Patienten erwarten, dass die behandelnde Ärztin oder der behandelnde Arzt Spezialisten anderer Disziplinen, die im Haus arbeiten, in die Behandlung einbindet. Von dem Einverständnis, dass der Fall auf einer Tumorkonferenz vorgestellt wird, ist daher auszugehen. Allein für den Fall, dass externe Ärztinnen und Ärzte an den Tumorkonferenzen teilnehmen, haben wir das Krankenhaus gebeten, die Patientinnen und Patienten hierüber zu informieren, da sie mit dieser Einbeziehung von externen Fachkräften nicht unbedingt rechnen und mögliche Einwände nicht geltend machen können.

144 Vgl. 8.2.3

Auch für die **Qualitätssicherung** der Behandlung, zu der das geprüfte wie jedes andere Krankenhaus gesetzlich verpflichtet ist, kann die Tumordokumentation unbedenklich eingesetzt werden, auch dann noch, wenn die behandelte Person bereits entlassen ist. Oft ist es hierfür nicht erforderlich, deren Namen zu kennen, insbesondere wenn die Behandlung bereits längere Zeit zurückliegt und die Daten nur zum Vergleich herangezogen werden. Für diesen häufigen Fall haben wir das Tumorzentrum aufgefordert, den Namen und weitere Angaben über die Patientin oder den Patienten, die die Identifizierung ermöglichen, zu löschen oder unumkehrbar durch ein Kennzeichen oder **Pseudonym** zu ersetzen.

Eine derartige Löschung oder Ersetzung ist auf jeden Fall geboten, wenn die behandelte Person bereits verstorben ist oder wenn die Daten für ein Forschungsvorhaben eingesetzt werden sollen. Werden die gleichen Daten – mit Pseudonymen versehen – zulässig in verschiedenen Forschungsvorhaben genutzt, so sind verschiedene, nicht aufeinander zurückführbare Pseudonyme zu verwenden. Wird in einem Forschungsprojekt die Kenntnis der Namen der Patientinnen oder Patienten ausnahmsweise benötigt, so bedarf es einer Einwilligung der Betroffenen, die sich auf das konkrete Projekt beziehen muss.

Bereits bei der Aufnahme werden die behandelten Personen von dem Krankenhaus um eine Einwilligung in die Datenübertragung an die Landestumorzentren von Berlin bzw. Brandenburg gebeten. Dies geschieht vorsorglich auch dann, wenn eine Krebserkrankung noch nicht vermutet wird. Die Einwilligung, die sich auf eine Situation bezieht, die die Patientin oder der Patient noch gar nicht überschauen kann, erstreckt sich daher nur auf eine eng begrenzte Verarbeitung der Patientendaten zur Unterstützung der qualitätssichernden Beurteilung der Behandlung des Krankenhauses durch das Landestumorzentrum. Für eine solche Beurteilung genügen pseudonymisierte Daten. Rückmeldungen des Landestumorzentrums an das Krankenhaus kann dieses anhand der Pseudonyme den Fällen zuordnen.

Um die Effektivität der Therapie einzuschätzen, beauftragt das Tumorzentrum das Landestumorzentrum zusätzlich damit, über eine **Melderegisteranfrage** zu ermitteln, ob die aus dem Krankenhaus entlassenen Patientinnen oder Patienten verstorben sind. Dies ist zulässig, es sind jedoch zwei Voraussetzungen zu beachten: Dieser Auftrag darf weder dazu führen, dass das Landestumorzentrum Pseudonyme in ihm für andere Zwecke übermittelten Daten aufdecken kann, noch dazu, dass das Landesamt für Bürger und Ordnungsangelegenheiten (LABO) erfährt, wer in Berlin an Krebs erkrankt ist. Wir haben uns im Zusammenhang mit der Novellierung des Krebsregister-Staatsvertrags zwischen den am Gemeinsamen Krebsregister beteiligten Ländern dafür eingesetzt, dass dieser **Abgleich im Gemeinsamen Krebsregister** als öffentlicher Stelle und ohne Datenübermittlung an das LABO durchgeführt wird.

Selbstverständlich müssen die äußerst sensitiven Gesundheitsdaten von Krebspatientinnen und -patienten sorgfältig vor der Offenbarung an Dritte geschützt werden, sowohl im Krankenhaus als auch bei der Übermittlung an das Landestumorzentrum. Wir mussten feststellen, dass bis zum Prüfungszeitpunkt die Übermittlungen an das Landestumorzentrum auf unverschlüsseltem Datenträger erfolgten. Bei einem Verlust des Datenträgers auf dem Transportweg bestand die Gefahr, dass die Daten einer großen Zahl von Krebskranken Dritten offenbart würden. Auf unseren Hinweis hin werden die Datenträger nunmehr verschlüsselt.

Innerhalb des Krankenhauses erschwert das von dem geprüften wie von vielen anderen Tumorzentren genutzte Gießener Tumordokumentationssystem allerdings erheblich, eine datenschutzgerechte differenzierte Einschränkung der Zugriffsmöglichkeiten auf die Daten in Abhängigkeit von den jeweils verfolgten Zwecken zu realisieren. Insbesondere scheint es nicht möglich, im Nachhinein zu ermitteln, wer wann die Akte einer Patientin oder eines Patienten in der Tumordokumentation eingesehen hat. Wir haben das Tumorzentrum aufgefordert, entweder in Kooperation mit dem Hersteller für eine Weiterentwicklung Sorge zu tragen oder zu einer anderen Dokumentationssoftware zu wechseln.

Der Aufbau einer klinischen Tumordokumentation bedarf sorgfältiger Unterscheidung zwischen der Nutzung der Daten, bei der die Kenntnis der Identität der Patientinnen und Patienten erforderlich ist, und solcher, bei der es genügt, anstelle der Namen mit Pseudonymen zu arbeiten. Die für die Dokumentation eingesetzte Technik muss diese Unterscheidung unterstützen und auch anderweitig das gleiche Sicherheitsniveau bieten wie die elektronische Patientenakte selbst.

8.3 Personalwesen

Aus der Praxis

Anamnesebogen

Der Presse entnahmen wir, dass das Land Berlin als Dienstherr und Arbeitgeber bei Einstellungsuntersuchungen einen Anamnesebogen (sog. Selbstauskunftsbogen) zur Erhebung von Gesundheitsdaten von Bewerberinnen und Bewerbern mit datenschutzrechtlich problematischen Fragen verwendete. So sollten die Betroffenen Fragen nach behandelnden Ärzten/Psychologen/Heilpraktikern, körperlichen Erkrankungen oder Unfällen, seelischen (psychischen) Erkrankungen und Therapien sowie Angaben zu Krankenhaus-/Kuraufenthalten/Operationen beantworten, ohne dass diese Fragen auf einen bestimmten Zeitraum begrenzt waren. Ebenso allgemein waren Fragen nach Drogenkonsum und Sport, dafür die vorgesehenen Antworten (nie; ab und zu; regelmäßig; abstinent seit) sehr detailliert. Die Datenerhebung erfolgt durch die Zentrale Medizinische Gutachtenstelle (ZMGA) beim Landesamt für Gesundheit und Soziales (LAGeSo). Der Bogen wird nicht Gegenstand der Personalakte. Er verbleibt in der ZMGA (Gesundheitsakte).

Die Datenerhebung, -speicherung und -nutzung muss zur Begründung des Arbeitsverhältnisses erforderlich sein.[145] Bei der Erhebung der Anamnesedaten durch die ZMGA handelt es sich um eine Datenerhebung durch den Dienstherrn bzw. in dessen Auftrag. Die Datenfelder und Fragen waren einer kritischen Betrachtung bezüglich der Erforderlichkeit zu unterziehen. Aufgrund unserer Interventionen wurde der Fragebogen geändert. Künftig werden die Betroffenen nur noch nach derzeit behandelnden Ärzten/Psychologen/Heilpraktikern befragt. Angaben zu körperlichen Erkrankungen oder Unfällen sowie Angaben zu seelischen (psychischen) Erkrankungen und Therapien und Angaben zu Krankenhaus-/Kuraufenthalten/Operationen sind nur noch für den Zeitraum der letzten zehn Jahre vorgesehen. Die Frage nach Drogenkonsum wurde konkretisiert. Hier sind jetzt nur noch Angaben zu Betäubungs- oder Aufputschmitteln vorgesehen. Die Frage nach regelmäßigem Sport ist nur noch mit Ja oder Nein zu beantworten. Dagegen sind Angaben zu Sportart und Stundenanzahl weggefallen.

145 § 2 Abs. 2 BlnDSG i. V. m. § 28 Abs. 1 Satz 1 Nr. 1 BDSG

Ferner ist das LAGeSo bzw. die ZMGA uns bezüglich des Hinweisblattes für die Betroffenen insoweit gefolgt, dass die Betroffenen keine Angaben im Bogen machen müssen, sondern die Fragen mit der Ärztin oder mit dem Arzt auch persönlich klären und besprechen können. Anforderungen von Befundberichten werden künftig nur nach Rücksprache bzw. Einverständnis der Betroffenen erfolgen. Die Frage nach sportlicher Betätigung wird den Betroffenen im Hinweisblatt erklärt. Bluttests werden grundsätzlich bei Angestellten nicht durchgeführt, bei Beamtinnen und Beamten nur nach Entscheidung der Ärztin oder des Arztes.

Der Selbstauskunftsbogen wird bei Beamtinnen und Beamten 30 Jahre, bei Angestellten zehn Jahre nach dem letzten Vorgang aufbewahrt und dann vernichtet. Der Bogen wird für alle Untersuchungen im Rahmen von Einstellungen und Prüfungen der Dienstfähigkeit verwendet. Bei der Justiz und im Polizeidienst werden andere Fragebögen verwendet, deren Überprüfung noch nicht abgeschlossen ist.

Der überarbeitete Anamnese-/Selbstauskunftsbogen bei Einstellungsuntersuchungen entspricht dem Grundsatz der Datensparsamkeit und Verhältnismäßigkeit. Zeitgleich wurden die Fragebögen zur Begutachtung nach dem SGB IX, dem Sozialen Entschädigungsrecht und dem Landespflegegeldgesetz im Rahmen der internen und externen Begutachtung von uns geprüft und datenschutzgerecht verändert.

Aus der Praxis

Übermittlung ärztlicher Gutachten an die Dienstbehörde

Trotz unserer mehrfachen Hinweise zur Übermittlung von Diagnosedaten von Beschäftigten durch die Amtsärztin bzw. den Amtsarzt an die Personalstelle erreichen uns immer wieder Beschwerden von Untersuchten.

Dies liegt zum einen an den Untersuchungsaufträgen der Personalstellen, die die Frage nach der Diagnose explizit enthalten[146], zum anderen an der Unsicherheit von Amtsärztinnen und -ärzten darüber, wie viel Informationen sie an die Personalstelle als Auftraggeberin weiterleiten müssen, um das Ergebnis ihrer Untersuchungen plausibel zu machen.

146 Rundschreiben I Nr. 11/2004 der Senatsverwaltung für Inneres und Sport

Die Feststellung der Dienstfähigkeit oder Dienstunfähigkeit von Beschäftigten durch die Dienstbehörde erfolgt aufgrund des ärztlichen Gutachtens. Die Entscheidung über die Dienstfähigkeit trifft jedoch allein die Dienstbehörde. Das ärztliche Gutachten selbst stellt keine Entscheidung dar, dient jedoch als Grundlage für eine sachgerechte Personalentscheidung der Dienstbehörde und muss deshalb nachvollziehbar sein. Dabei darf die Ärztin oder der Arzt im Einzelfall auf Anforderung der Dienstbehörde das die tragenden Feststellungen und Gründe enthaltende Gutachten mitteilen, soweit deren Kenntnis für die Dienstbehörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist.[147]

Dies bedeutet, dass grundsätzlich zunächst nur mitgeteilt werden darf, ob die Beschäftigten uneingeschränkt dienstfähig oder dienstunfähig sind. Bei **eingeschränkter Dienstfähigkeit** sind der Personalstelle nur die gesundheitsbedingten Leistungseinschränkungen mitzuteilen. Dagegen muss die Dienstbehörde bei Versetzungen in den Ruhestand den Betroffenen in ihrer Entscheidung die Tatsachen, auf die sie ihre Entscheidung stützt, so nachvollziehbar (bei Beamtinnen und Beamten als Adressat eines Verwaltungsaktes) mitteilen, dass diese in ihrer Rechtswahrung nicht eingeschränkt sind.

Wir haben die Senatsverwaltung für Inneres und Sport daher gebeten, ihr Rundschreiben entsprechend zu ändern und in den Untersuchungsauftrag eine Formulierung aufzunehmen, nach der die Angabe der Diagnosedaten nur für den Fall unaufgefordert erfolgen kann, soweit vollständige Dienstunfähigkeit aus medizinischer Sicht festgestellt wurde. Die Senatsverwaltung hat uns die Änderung des Rundschreibens zugesagt.

Die Übermittlung nicht erforderlicher Diagnosedaten durch die Ärzteschaft an die Dienstbehörde bedeutet eine Verletzung der Verschwiegenheitspflicht und kann strafbar sein.

147 § 45 Abs. 1 LBG

Übermittlung von Beschäftigtendaten an Konzernmutter in den USA

Ein Mitarbeiter eines großen Unternehmens hatte sich mit dem Hinweis an uns gewandt, sein Arbeitgeber würde Personaldaten in die USA übermitteln und dort speichern. Das Unternehmen bestätigte diese Aussage und teilte mit, die gesamte Datenverarbeitung fände bei der Konzernmutter in den USA statt. Das Unternehmen sei jedoch dem Safe Harbor-Abkommen beigetreten. Im Übrigen sei den Beschäftigten die Datenübermittlung bekannt.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit der Betroffene eingewilligt hat oder eine Rechtsvorschrift dafür besteht.[148] Die Wirksamkeit der Einwilligung scheitert bei Arbeitsverhältnissen wegen der sozialen Abhängigkeit an der Freiwilligkeit. Es reicht auch nicht aus, dass die Datenübermittlung in die USA allen Beschäftigten bekannt war, da Transparenz keine die Datenübermittlung rechtfertigende Rechtsvorschrift ersetzt.

Da derartige Übermittlungen von teilweise sogar sensitiven Daten (z. B. über die Gesundheit) nicht erforderlich sind, ist eine **Datenverarbeitung im Auftrag** des deutschen Unternehmens durch die Konzernmutter denkbar. Doch auch diese **bedarf einer Rechtsvorschrift,** da es sich bei der Konzernmutter in den USA um ein Unternehmen in einem Drittland handelt.[149]

Die Datenverarbeitung in den USA könnte in der sog. 1. Stufe eine Betriebsvereinbarung regeln.[150] Diese stellt eine Rechtsvorschrift dar. Allerdings ist eine Betriebsvereinbarung nur dann wirksam, wenn sie nicht zu einer Verringerung des gesetzlich vorgegebenen datenschutzrechtlichen Niveaus führt. Die Betriebsvereinbarung muss deshalb **gleichwertige Schutzvorkehrungen wie das Bundesdatenschutzgesetz** enthalten. So müssen die Betroffenen das Recht erhalten, alle Ansprüche (z. B. auf Auskunft, Schadensersatz wegen Datenschutzverstößen in den USA) auch gegenüber ihrem Arbeitgeber geltend machen zu können. Als weitere flankierende Maßnahme sollte das Unternehmen ähnlich verpflichtet und kontrolliert werden wie ein Auftragsdatenver-

148 § 4 BDSG
149 § 3 Abs. 8 BDSG
150 Zur Wirkung von Betriebsvereinbarungen in der sog. 1. sowie 2. Stufe vgl. JB 2002, 4.7.3 (a. E.)

arbeiter nach § 11 BDSG. Durch diese zusätzlichen Sicherungsmaßnahmen ist gewährleistet, dass die schutzwürdigen Interessen der Beschäftigten gegenüber dem wirtschaftlichen Interesse der verantwortlichen Stelle an der Datenübermittlung nicht überwiegen.

Im Hinblick auf die sog. 2. Stufe ist hervorzuheben, dass sich der deutsche Datenexporteur bei einer Safe Harbor-Zertifizierung der Konzernmutter nicht mehr auf die bloße Behauptung verlassen kann, sie behandele die personenbezogenen Daten nach den Grundsätzen des Safe Harbor-Abkommens. Hier trifft den Datenexporteur eine gewisse **Prüfpflicht.**[151]

Trotz Safe Harbor-Zertifizierung des Daten importierenden US-Unternehmens ist eine Auftragsdatenverarbeitung nur bei Vorliegen einer Rechtsvorschrift (z. B. einer Betriebsvereinbarung) zulässig.

8.4 Wohnen und Umwelt

8.4.1 Datenschutz und Denkmalschutz in der Hufeisensiedlung

Die Hufeisensiedlung in Berlin–Britz gehört zum UNESCO Weltkulturerbe. Der Verein der Freunde und Förderer der Hufeisensiedlung Berlin-Britz e. V. und das Landesdenkmalamt entwickelten deshalb die Idee einer Denkmalschutzdatenbank. Beabsichtigt ist, denkmalpflegerische Gutachten und eine Datenbank zum Gebäudebestand zu veröffentlichen. Der Baubestand soll in Form von Zeichnungen wiedergegeben werden, die den Altzustand zeigen und einzelnen Häusern nach Straße und Hausnummer zugeordnet sind. Ein Ziel der Datenbank ist, dabei zu helfen, den abgebildeten ursprünglichen Zustand mit künftigen Umbauten wieder zu erreichen. Dafür sollen u. a. die Flächen von Haus und Grundstück, Wohnflächengrundrisse, Türen- und Fensterbestand, Farben sowie der Baumbestand abgebildet werden.

151 Vgl. 11.2

Aus den geplanten Veröffentlichungen ergeben sich Informationen über die Wohn- und Eigentumsverhältnisse der Mieterinnen und Mieter sowie Eigentümerinnen und Eigentümer. Diese sind aufgrund der Suchmöglichkeit nach Hausnummern bestimmbar. Die Abbildungen z. B. von Grundrissen oder dem ursprünglichen Zustand in den Fällen, in denen dieser der aktuellen Architektur entspricht, enthalten Angaben über sachliche Verhältnisse der Betroffenen. Aktuelle Wohnverhältnisse werden also bekannt, soweit individuelle Eigenschaften auch heute noch identisch, unverändert, dauerhaft oder unveränderbar sind.

Um den Schutz der Betroffenen zu gewährleisten, haben wir empfohlen, ihnen ein Widerspruchsrecht einzuräumen, wenn die Datenbank öffentlich zugänglich wird.[152] Die Betroffenen erhalten dadurch die Möglichkeit, der Veröffentlichung entgegenzutreten. Solange sie ihr nicht widersprechen, können die Daten verwendet und veröffentlicht werden.[153] Wichtig ist dabei, dass die Berechtigten auf die Widerspruchsmöglichkeit hingewiesen werden.

Ähnlich wie bei Google Street View[154] und dem Solarflächen-Potenzialatlas[155] haben Gebäudeeigentümer und -bewohner auch bei einer Denkmalschutzdatenbank das Recht, der Veröffentlichung von Informationen zu ihren Häusern und Grundstücken zu widersprechen.

8.4.2 Baulückenmanagement

Die Berlin Partner GmbH betreibt ein 3D-Stadtmodell. In einem dreidimensionalen Spaziergang vermittelt das Modell Interessenten und Investoren ein Bild über Lage und Umgebung von Berliner Adressen. Zur Verfügung stehen eine Version, die intern zur Beratung von Investoren genutzt wird, sowie eine öffentlich zugängliche Version über Google Earth.

152 Bislang ist die Datenbank nur behördenintern verfügbar.

153 Diese sog. „Opt Out"-Lösung stützt sich auf § 6 Abs. 1 S. 2 BlnDSG. Sie stellt den bestmöglichen Ausgleich zwischen den Dokumentations- und Informationsinteressen einerseits und den schutzwürdigen Belangen der Betroffenen andererseits her. Zulässig wären aber auch andere Lösungsansätze wie eine geschlossene Benutzergruppe oder der Verzicht auf den genauen Adressbezug.

154 Vgl. 1.1.2

155 Vgl. 8.4.3

Von der Senatsverwaltung für Stadtentwicklung wird eine Datenbank für das Baulückenmanagement bereitgestellt. Hier haben Interessierte die Möglichkeit, verfügbare Bauflächen zu recherchieren und sich diese auf Karten anzeigen zu lassen. Enthalten sind Informationen wie Straße, Flurstücksnummer und ob die Eigentümerinnen oder Eigentümer das Land Berlin oder Privatpersonen sind.

Die Senatsverwaltung und die Berlin Partner GmbH hatten den Wunsch, die beiden Angebote zu verbinden, und baten uns dazu um Rat. Im 3D-Stadtmodell sollten die Potenzialflächen kenntlich gemacht werden, indem die Fläche im 3D-Stadtmodell mit der Baulückenmanagementdatenbank verknüpft wird. Bei der freien Fläche im Stadtmodell sollte für diesen Zweck ein Datenblatt mit Angaben zum Bauland angezeigt werden.

Über das 3D-Stadtmodell werden zusätzliche Verknüpfungen automatisch erstellt. So sind weitere statistische Daten wie z. B. Informationen zum Denkmalschutz, zum Sozialgefüge der Umgebung und zu angesiedelten Wirtschaftsunternehmen einsehbar. Durch die Verbindung des Baulückenmanagements mit dem 3D-Stadtmodell würde das Baulückenmanagement indirekt daher auch mit diesen zusätzlichen Informationen verknüpft.

Diese Verknüpfung ist nach der geltenden Rechtslage unzulässig[156]. Zwar dürften die flächenbezogenen Angaben der Baulückendatenbank mit Luftbildern und Fotos der Umgebung der Baulücken u. U. zusammengeführt werden. Eine Verknüpfung mit den über das 3D-Stadtmodell abrufbaren weiteren statistischen Daten ist hingegen nicht rechtmäßig. Denn bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich um personenbezogene Daten. Auch durch eine Anreicherung der im Baulandkataster enthaltenen Daten mit weiteren statistischen Daten ließe sich zumindest eine Personenbeziehbarkeit ableiten.

156 Maßgeblich sind insbesondere § 200 Abs. 3 BauGB und § 2 Abs. 2 Baulückenmanagement-Abrufverordnung des Landes Berlin.

Eine Verknüpfung von Informationen des Baulandkatasters mit dem 3D-Stadtmodell, über das weitere statistische Stadtplanungsdaten abrufbar sind, ist derzeit nicht zulässig. Entsprechend unserem Rat haben die beteiligten Stellen davon Abstand genommen, diese Verknüpfung online abrufbar zu machen.

8.4.3 Solarflächen-Potenzialatlas

Die Berlin Partner GmbH betreibt einen Solarflächen-Potenzialatlas, bei dem sich Interessierte darüber informieren können, ob das Dach eines Gebäudes für die Nutzung von Solarenergie geeignet ist. Hier wird gebäudescharf das Solarpotenzial der Stadt gezeigt. Mögliche Stromerzeugung, CO_2-Einsparung und Investitionskosten werden im Modell anhand von farbigen Säulen sichtbar. Das Modell wendet sich insbesondere an Immobilieneigentümer und Investoren.

Den Solaratlas kann jedermann nutzen, der über einen Internetzugang verfügt. Eine öffentliche Version in 3D steht über Google Earth zur Verfügung. Außerdem gibt es ein 3D-Modell für den internen Gebrauch der Senatsverwaltung für Stadtentwicklung und der Berlin Partner GmbH, das noch mehr Details präsentiert. Der Solaratlas nutzt dabei das vorhandene 3D-Stadtmodell des Landes Berlin, das auf dem amtlichen Kataster basiert.

Dabei sind alle Daten, die als personenbezogen anzusehen sind, wie Kfz-Kennzeichen, Personenabbildungen oder Namensschilder von Personen an Gebäuden, vor der öffentlichen Nutzung unkenntlich zu machen. Zudem sind die Betroffenen in dem Internetauftritt darauf hinzuweisen, dass sie ihr Recht auf informationelle Selbstbestimmung durch Widerspruch geltend machen können. Neben Haus- und Wohnungseigentümern gehören z. B. auch Mieter, Pächter und Bewohner im Allgemeinen zum Kreis der Betroffenen. Wenn sie der Abbildung widersprechen, darf das Gebäude, in dem sie wohnen oder das ihnen gehört, nicht öffentlich dargestellt werden.

Die Berlin Partner GmbH hat dementsprechend einen Hinweis zu ihrem 3D-Stadtmodell aufgenommen, mit dem Betroffene auf die Möglichkeit aufmerksam gemacht werden, der Darstellung ihres Gebäudes zu widersprechen. Zudem sind personenbezogene Darstellungen wie Bilder von Personen und Kfz-Kennzeichen im 3D-Stadtmodell unkenntlich zu machen.

9. Wissen und Bildung

9.1 Wissenschaft, Forschung und Statistik

9.1.1 Datenschutzrichtlinie der Freien Universität Berlin

Das Präsidium der Freien Universität Berlin (FUB) hat zur Regelung des hochschulinternen Datenschutzes die sog. „Datenschutzrichtlinie“ erlassen. Bei einer Richtlinie handelt es sich um eine Verwaltungsvorschrift, die nur eine interne Selbstbindung der Verwaltung bewirkt. Zur Regelung datenschutzrechtlicher Aspekte ist jedoch ein Gesetz im materiellen Sinne erforderlich, also eine Rechtsnorm mit unmittelbarer Außenwirkung. Dieses Erfordernis ergibt sich aus dem insoweit eindeutigen Wortlaut des Berliner Datenschutzgesetzes[157]. Danach ist die Verarbeitung personenbezogener Daten u. a. nur dann zulässig, wenn eine besondere Rechtsvorschrift, beispielsweise eine Satzung, sie erlaubt. Das ist auch deshalb sachgerecht, weil es um die Begrenzung von Eingriffen in die Grundrechte von Angehörigen der Hochschule geht. Die Regelung des Datenschutzes durch eine Verwaltungsvorschrift ist mithin unzulässig.

Der Akademische Senat der FUB ist demzufolge gehalten, von seiner Satzungsbefugnis nach dem Berliner Hochschulgesetz Gebrauch zu machen und eine Satzung zur Verarbeitung personenbezogener Daten zu erlassen[158]. Bis dahin findet bezüglich des hochschulinternen Datenschutzes das Berliner Datenschutzgesetz Anwendung.

Die Regelung datenschutzrechtlicher Aspekte in Form einer Richtlinie ist unzulässig. Es obliegt dem Akademischen Senat der FUB, eine Datenschutzsatzung zu erlassen. Solange sie nicht existiert, ist das Berliner Datenschutzgesetz auf den Datenschutz in der Hochschule anwendbar.

157 § 6 Abs. 1 Satz 1 BlnDSG
158 § 61 Abs. 1 Nr. 4 BerlHG

9.1.2 RFID-gestützte Zugangskontrollsysteme an Hochschulen

Wenn der Bedarf zur Modernisierung der Schließsysteme in öffentlichen Stellen des Landes erkannt wird, liegt es nahe, eine Entscheidung für ein RFID-gestütztes Zugangskontrollsystem zu treffen. Bei solchen Schließsystemen erfolgt das Öffnen und Schließen der Türen kontaktlos über einen **RFID-Transponder.**

Es gibt einige Argumente, die dafür sprechen, von einer solchen mechanischen Schließanlage zu einer elektronischen umzurüsten. Dieser Wechsel vereinfacht die Schlüsselverwaltung und verringert die Missbrauchsgefahr erheblich. Zu den Vorteilen elektronischer Schließsysteme gehören die mögliche Realisierung sich überschneidender Gruppenschließungen und die deutliche Erschwernis nicht autorisierter Schlüsselvervielfältigung. Die individuellen Zutrittsrechte von Personen, die mit einem solchen Schlüssel ausgestattet werden, können flexibel auf dem Transponder abgelegt werden, sodass die Personen nur die Türen passieren können, durch die sie gehen sollen, und jene verschlossen bleiben, hinter denen sie nichts zu suchen haben. Bei Verlust eines Transponders können einfach die entsprechenden Schlösser für diesen Transponder gesperrt werden. Es müssen daher weder alle Schlüssel und Schlösser noch die gesamte Schließanlage ausgetauscht werden. Eine elektronische Schließanlage erhöht also die Sicherheit (auch der Datenverarbeitungsanlagen und Datenträger in verschlossenen Bereichen), die Flexibilität der Administration und senkt die Betriebskosten.

Datenschutzrechtlich relevant werden solche Schließsysteme, aber auch jene, die mit anderen **maschinenlesbaren Ausweisen oder Tokens** arbeiten, vor allem, wenn die Nutzung solcher Schlüssel protokolliert wird und somit die Möglichkeit besteht, zumindest im eingeschränkten Maße **Bewegungsprofile** der Zutrittsberechtigten innerhalb der Räume der anwendenden Stelle zu erstellen. Wie genau diese Profile sind, hängt davon ab, wie differenziert die Zugriffsberechtigungen vergeben sind, welche Türen also mit dem Schlüssel geöffnet werden müssen und damit kontrolliert werden können, und was im Einzelnen bei jeder Nutzung protokolliert wird, z. B. Ort der Tür, Zeitpunkt ihrer Öffnung und Rolle der berechtigten Person.

Bei RFID-Systemen kommt hinzu, dass die Kommunikation zwischen Chip und den Endgeräten des Schließsystems über **Funkwellen** stattfindet. Die Protokollierung der Nutzung kann auf den Chips selbst, in den Endgeräten des Schließsystems und/oder in den zentralen Einrichtungen (z. B. Server) des Schließsystems erfolgen. Es besteht bei der Funkwellenkommunikation ferner das Risiko, dass Unbefugte den Funkverkehr mit eigenen Empfängern verfolgen und so illegal Bewegungsprofile erstellt werden können[159].

Sofern RFID-gestützte Schließsysteme personenbezogene Daten verarbeiten, sind sie als automatisiertes Datenverarbeitungsverfahren zu betrachten. Im Geltungsbereich des Berliner Datenschutzgesetzes (BlnDSG) hat dies zur Folge, dass zur Einschätzung der oben dargestellten Risiken nach § 5 Abs. 3 Satz 1 BlnDSG eine **Risikoanalyse** und darauf aufbauend ein **Sicherheitskonzept** erstellt werden muss, das sich auch auf die personenbezogene Stammdatenverwaltung in den zentralen Komponenten, vor allem aber auf die Protokollierungsfunktionen beziehen und die speziellen sicherheitsrelevanten Eigenschaften von Funkchips berücksichtigen muss. Da es sich in der Regel um Personaldaten handelt, die in dem Verfahren verarbeitet werden und die dem besonderen Personalaktengeheimnis unterliegen können, könnte nach § 5 Abs. 3 Satz 2 BlnDSG auch eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten geboten sein. Grundlagen einer solchen **Vorabkontrolle** sind regelmäßig die Dateibeschreibung nach § 19 BlnDSG, die alle rechtlich prüfbedürftigen Informationen enthalten sollte, sowie das erwähnte Sicherheitskonzept einschließlich der Risikobetrachtungen.

Anlass zur Befassung mit RFID-gestützten Schließsystemen waren die Projekte zur Einführung solcher Systeme in zwei Berliner Hochschulen, der Freien Universität Berlin (FUB) und der Hochschule für Wirtschaft und Recht (HWR). Dabei steht das Verfahren bei der FUB unmittelbar vor seiner Einführung, während sich das Projekt der HWR erst im Anfangsstadium befindet. Gemeinsam ist beiden Hochschulen, dass der Betrieb der elektronischen Schließsysteme als Datenverarbeitung im Auftrag durch externe Auftragnehmer durchgeführt wird und somit in beiden Fällen die Auftragsvergabe nach § 3 BlnDSG geregelt werden muss.

159 Vgl. auch 12.3

Freie Universität Berlin

Die FUB hat 2008 mit dem Projekt begonnen, in ihren Häusern die mechanischen Schließanlagen durch ein elektronisches Schließsystem zu ersetzen. Die Beschäftigten erhalten die Zugangsberechtigungen zu den einzelnen Bereichen mit Hilfe von RFID-Transpondern, die in Schlüsseletiketten integriert sind. Die Bereiche werden je nach Bedarf mit Online- bzw. Offline-Schlössern gesichert.

Bei den Online-Schlössern ist die Berechtigung der Transponder auf dem zentralen Server der **Zutrittskontrollzentrale (ZKZ)** gespeichert. Jedes Schließen oder Öffnen eines Online-Schlosses wird protokolliert und auf dem zentralen Server für sechs Monate im Ringspeicherverfahren gespeichert. Der Zugriff auf diese Protokolldaten ist nur nach dem Vier-Augen-Prinzip möglich, was in der Dateibeschreibung ausführlich erläutert wird.

Die Offline-Schlösser hingegen haben einen internen Speicher, in dem festgehalten ist, welche der Transponder-Identifikationsnummern dazu berechtigt sind, dieses Schloss zu öffnen. Die Speicherung des Schließens bzw. Öffnens erfolgt lokal im jeweiligen Endgerät (Schloss). Es werden maximal 500 Schließungen/Öffnungen protokolliert und im Ringspeicherverfahren gespeichert. Bei einem solchen Verfahren wird nach Füllung des Speichers für jeden neuen Eintrag der älteste vorhandene Eintrag gelöscht. Der Zugriff auf diese Protokolldaten ist ebenfalls nur nach dem Vier-Augen-Prinzip möglich.

Unter diesen Umständen haben wir trotz der theoretischen Möglichkeit der Erstellung von Bewegungsprofilen die Missbrauchsgefahr als gering eingestuft. Die einzig zugangsberechtigten Personen – der zentrale Administrator und ein sog. Zutrittskontrolleur – können nur gemeinsam eine Auswertung der Daten und damit eine Personenzuordnung vornehmen.

Die grundlegenden Risiken, die im Falle der FUB abgeschätzt wurden, sind der Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit der im Verfahren verarbeiteten personenbezogenen Daten. Bei einem Diebstahl oder Verlust eines Transponders hat dies keine Auswirkungen auf die Vertraulichkeit, da auf ihm keine personenbezogenen Daten gespeichert werden und die abgelegten Betriebsdaten verschlüsselt sind. Die Integrität der Transponderdaten ist gewährleistet, da sie sicher verschlüsselt werden und in diesem

Zustand nicht gezielt verändert werden können. Der Ausfall des Systems, z.B. wegen fehlender Verfügbarkeit der Daten, kann zur Folge haben, dass der Zugang zum Gebäude nicht mehr möglich ist. Das Verlassen des Gebäudes ist jederzeit auch ohne Transponder (zumindest über die Fluchttüren) möglich, denn ersatzweise können alle mit einer elektronischen Schließung versehenen Außentüren im Notfall auch mit einem mechanischen Schlüssel geöffnet werden.

Da die FUB die zentrale Verwaltung des Schließsystems einer Fremdfirma übertragen hat, kann nur die Firma in Absprache mit der FUB Schließrechte an neue Hochschulangehörige vergeben. Damit verbundene Missbrauchsrisiken müssen bei der vertraglichen Regelung der Auftragsdatenverarbeitung nach § 3 Abs. 1 und 4 BlnDSG hinreichend berücksichtigt werden. Dies ist bisher noch nicht geschehen.

Hochschule für Wirtschaft und Recht

An der HWR wurden die mit der Modernisierung der Schließanlage eingehenden Fragestellungen erst in einer späten Phase problematisiert. Es ist also noch zu wenig über das System bekannt, als dass hier darauf eingegangen werden könnte. Neben den bereits beschriebenen allgemeinen Problemfeldern, die noch zu klären sind, kommt auch hier die Besonderheit hinzu, dass die Administration des Systems der privaten Hausverwaltung übertragen wird.

Wie viele Behörden ist die HWR lediglich Mieterin der Campusgebäude, die durch die Berliner Immobilienmanagement GmbH (BIM) für das Land Berlin verwaltet werden. Die Hausverwaltung wird durch eine privatrechtliche Gesellschaft im Auftrag der BIM wahrgenommen. Der Betrieb der elektronischen Schließanlage soll zukünftig durch diese Hausverwaltung übernommen werden. Es handelt sich in diesem Fall um eine Verarbeitung personenbezogener Daten im Auftrag, die nach § 3 BlnDSG grundsätzlich zulässig ist, wenn vertraglich geregelt wird, dass der Auftragnehmer die Vorschriften des BlnDSG befolgt und sich unserer Kontrolle unterwirft. Die sichere Administration und der datenschutzkonforme Umgang mit den personenbezogenen Daten der Beschäftigten der HWR muss daher in den Weisungen der Auftraggeberin, die Vertragsgegenstand sein müssen, konkret beschrieben werden.

Die Einführung elektronischer Schließsysteme kann die Datensicherheit erhöhen. Der Umstand, dass im Gegensatz zu herkömmlichen Schließanlagen in den meisten Fällen jedoch auch datenschutzrechtliche Problemfelder wie die Bildung von Bewegungsprofilen berührt werden, macht eine diesbezügliche Planung durch die betroffenen Stellen für einen datenschutzgerechten Betrieb unausweichlich. Sowohl bei der FUB als auch bei der HWR wird die Erfüllung datenschutzrechtlicher Anforderungen wesentlich davon abhängen, wie die Auftragsvergabe nach § 3 Abs. 1 und 4 BlnDSG an private Dienstleistungsunternehmen dazu die notwendigen Rahmenbedingungen sicherstellt.

9.1.3 Forschungsprojekt myID.privat

Wir haben uns beratend an einem Forschungsprojekt der Technischen Universität Berlin, des Fraunhofer Instituts FOKUS sowie der Bundesdruckerei beteiligt.

Ziel des Projektes „myID.privat“ ist es, einerseits die Sicherheit und andererseits die Kontrolle der Nutzenden über die Weitergabe ihrer personenbezogenen Daten bei rechtsverbindlichen Aktivitäten im Internet zu verbessern. Dazu wird eine entsprechende Technologie anhand beispielhafter Anwendungsszenarien entwickelt. Konkrete Szenarien, die gemeinsam mit Behörden- bzw. Industriepartnern evaluiert wurden, sind z. B. das Erstatten einer **Online-Anzeige bei der Polizei,** das **Beantragen einer Kfz-Versicherung** oder die nutzerkontrollierte **Übermittlung von Bonitätsbewertungen** von und zu Auskunfteien. Neben bestimmten Identitätsdaten der Beteiligten, für die im Projekt die eID-Funktionalität des neuen Personalausweises genutzt wird[160], sind je nach Szenario noch weitere Nachweise zu erbringen. Für die Kfz-Versicherung ist beispielsweise die Anmeldebestätigung des Pkw sowie ggf. der Nachweis eines Garagenparkplatzes erforderlich.

Das Projekt bezweckt nun, den Antragstellenden die Möglichkeit zu geben, entsprechende Nachweise elektronisch einzuholen und an die jeweils anderen

160 Vgl. 2.4

Partner weiterzugeben. Dabei soll so datensparsam wie möglich gearbeitet werden: Die Ersteller entsprechender Nachweise erfahren nicht, für welchen Zweck bzw. gegenüber welchem Anbieter der Nachweis genutzt wird. Auch der Empfänger eines Nachweises soll nur die wirklich notwendigen Informationen erhalten, z. B. dass ein Garagenstellplatz existiert, nicht jedoch, wer diesen vermietet. Zudem werden alle personenbezogenen Daten erst bei Vertragsabschluss und nach der Möglichkeit der Prüfung durch den Antragstellenden an den jeweiligen Vertragspartner übermittelt.

Bei einigen Szenarien konnten wir weitere datenschutzfreundliche Optionen einbringen. So könnten Betroffene interessiert sein, ihren von Auskunfteien berechneten Bonitäts-Scorewert zu verbessern, indem sie der jeweiligen Auskunftei bisher unbekannte Positivdaten wie das Vorhandensein eines Arbeitsplatzes oder den Besitz einer Immobilie mitteilen. Unsere Anforderungen an ein solches Verfahren lauten u. a., dass vor der Datenübermittlung ein **anonymer Test** möglich sein muss, ob die zu übermittelnden Daten die von der jeweiligen Auskunftei berechnete Bonität der Betroffenen überhaupt verbessern.

Ein weiterer Aspekt des Forschungsprojektes ist, den Nutzenden eine möglichst verständliche Übersicht der zu übermittelnden Daten und der spezifischen Risiken zu geben. An einer prototypischen Implementierung der Nutzerschnittstelle wurde beispielsweise eine erweiterte Ampelkennzeichnung getestet, die aufzeigt, wie sensitiv bestimmte Kombinationen von personenbezogenen Daten und deren Zweckbestimmung sein können, die an einen Vertragspartner übermittelt werden. Insbesondere bei einigen der in einem Teilprojekt analysierten Kundenbindungsprogramme mit Kundenkarten würde eine derartige **Ampelkennzeichnung** dazu beitragen, den Nutzenden die erheblichen Risiken für die Privatsphäre aufgrund des oft großen Datenumfangs und der wenig beschränkten Zweckbindung zu verdeutlichen, und wahrscheinlich zu einem bewussteren Umgang mit derartigen Kundenkarten führen.

Datenschutz kann gerade im Internetzeitalter nicht allein durch (nationale) Gesetze sichergestellt werden. Notwendig ist auch die Entwicklung und Verbreitung von datenschutzfreundlichen Technologien für praktische Anwendungsfälle. Deutsche Unternehmen, die entsprechende Dienste oder Produkte anbieten, könnten dadurch Vorteile im internationalen Wettbewerb erlangen.

9.1.4 Zensus 2011 – Stand der Vorbereitung

2011 wird erstmals seit langem wieder eine Volkszählung stattfinden, der Zensus 2011. Ziel ist die Ermittlung der aktuellen Einwohnerzahlen. Sie werden u. a. für staatliche und kommunale Planungen, den Finanzausgleich, die Sitzverteilung im Bundesrat und als Fortschreibungsbasis für weitere Statistiken benötigt. Anders als bei den Volkszählungen 1987 (für die damalige Bundesrepublik) bzw. 1981 (für die damalige DDR) handelt es sich diesmal nicht um eine Totalerhebung. Haushaltsbefragungen wird es nur in Stichproben geben. Die Zählung basiert insbesondere auf Daten, die aus den Melderegistern und erwerbsstatistischen Registern der Bundesagentur für Arbeit und weiterer nach dem Finanz- und Personalstatistikgesetz auskunftspflichtiger Stellen stammen. Daher spricht man auch von einer registergestützten Volkszählung, bei der bereits vorhandene Daten zusammengeführt werden. Für Berlin werden die Daten aus den Melderegistern zunächst an das Amt für Statistik Berlin–Brandenburg gegeben, das sie an das Statistische Bundesamt übermittelt.

Daneben gibt es eine **Gebäude- und Wohnungszählung,** bei der alle Eigentümerinnen und Eigentümer von Wohnraum schriftlich befragt werden. Hierbei werden Angaben zu den Gebäuden und Wohnungen wie Eigentumsverhältnisse, Baujahr und Wohnfläche schriftlich erfragt. Auch in Gemeinschaftsunterkünften findet eine Vollerhebung statt. Im Herbst versandte das Amt für Statistik Berlin–Brandenburg für die Vorbereitung der Gebäude- und Wohnungszählung Informationsschreiben mit Rückmeldebogen an etwa 170.000 Eigentümerinnen und Eigentümer. Im Rahmen dieser Vorerhebung wurden zur Klärung der Auskunftspflicht die Anschriften und Eigentumsverhältnisse von Wohnungen und Gebäuden geprüft und aktualisiert. Diese Klärung erleichtert den Statistikerinnen und Statistikern anschließend die Organisation der Haupterhebung für die Gebäude- und Wohnungszählung, die im Mai 2011 auf Basis der gewonnenen Aktualisierungen stattfinden wird.

Ab Mai 2011 werden zudem **Haushaltsstichproben** durchgeführt. Dazu werden sog. Erhebungsbeauftragte (Interviewer) die zu befragenden Haushalte aufsuchen und die Fragebögen übergeben bzw. (soweit gewünscht) mit den Auskunftspflichtigen ausfüllen. Etwa 4 % der Berlinerinnen und Berliner sollen auf diese Weise befragt werden. Der Fragebogen kann auch online ausgefüllt werden.

Diejenigen, die aufgefordert werden, für den Zensus 2011 Angaben zu machen, sind grundsätzlich zur Auskunft verpflichtet. Dies ist gesetzlich festgelegt.[161] Freiwillig ist jedoch die Beantwortung der Frage nach dem Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung. Die erhobenen Daten dienen nur statistischen Zwecken, sie werden nicht an andere Behörden weitergegeben oder zu anderen Zwecken verwendet. Eine Rückübermittlung an die Verwaltungsbehörden ist durch das Zensusgesetz 2011 ausdrücklich untersagt. Dies entspricht den Vorgaben des Bundesverfassungsgerichts von 1983[162].

Lange Zeit umstritten war die Frage, wie mit **Übermittlungssperren** umzugehen ist, die in den Melderegistern gespeichert sind, wenn für den Betroffenen eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange zu befürchten ist.[163] Aufgrund der Entscheidung des Bundesgesetzgebers übermitteln die Meldebehörden den statistischen Ämtern der Länder Übermittlungssperren und den Grund der Übermittlungssperren.[164] Wie im weiteren Verlauf mit diesen Meldedatensätzen zu verfahren ist, lässt das Gesetz jedoch offen. Das Bundesinnenministerium und das Statistische Bundesamt vertraten zunächst die Auffassung, die Personen mit Übermittlungssperren müssten, soweit sie unter einer Anschrift gemeldet seien, die Teil der Stichprobe werde, zu ihrem Schutz von der Befragung ausgenommen werden. Die Landesstatistikämter und die Landesdatenschutzbeauftragten haben demgegenüber darauf hingewiesen, dass ein solches Vorgehen die Gefahr für die Betroffenen erhöhe, weil neben den Erhebungsbeauftragten auch noch weitere Personen über die Übermittlungssperren informiert werden müssten. Die Landesbehörden, die ohnehin für die Durchführung des Zensusgesetzes zuständig sind, setzten sich deshalb dafür ein, dass Personen mit Übermittlungssperren, soweit sie Teil der Haushaltsstichprobe seien, wie alle anderen Auskunftspflichtigen in die Zählung einbezogen werden. Weder die Erhebungsstellen noch die Erhebungsbeauftragten werden von Übermittlungssperren in Kenntnis gesetzt. Nur auf diese Weise können die Personen mit Übermittlungssperren vor zusätzlichen Gefährdungen geschützt werden. Diesem richtigen Standpunkt hat sich der Bund nach dem Ende des Berichtszeitraums schließlich angeschlossen.

161 § 18 ZensG 2011
162 BVerfGE 65, 1 ff. (Volkszählung)
163 Nach § 28 Abs. 5 Satz 2 MeldeG ist eine Melderegisterauskunft grundsätzlich unzulässig, solange eine Gefahr für den Betroffenen nicht ausgeschlossen werden kann.
164 § 3 Abs. 1 Nr. 26 ZensG 2011

Von Anfang an waren wir in die Planungen des Amtes für Statistik Berlin–Brandenburg zur Durchführung des Zensus 2011 einbezogen. Wir kontrollieren dort das Sicherheitskonzept und den Prozess der Datenverarbeitung, um ein hohes Schutzniveau sicherzustellen.

9.2 Schule

9.2.1 Automatisierte Schülerdatei

Im September 2007 teilte die Senatsverwaltung für Bildung, Wissenschaft und Forschung in einer Pressemitteilung mit, dass in Berlin eine *„zentrale Schülerdatenbank"* aufgebaut werden soll, *„um exakte Planungsdaten zur Verfügung zu haben"*. Unser Angebot, das Projekt datenschutzrechtlich zu begleiten, wurde von der Senatsverwaltung aufgegriffen, nachdem sich die Pläne für eine derartige Datei konkretisiert hatten.

Mit dem Gesetz zur automatisierten Schülerdatei von 2009[165] wurden Regelungen zur Einrichtung und Führung einer entsprechenden Datei in das Berliner Schulgesetz (SchulG) eingefügt. Auf der Grundlage des neuen § 64 a Abs. 1 SchulG ist die Senatsverwaltung für Bildung, Wissenschaft und Forschung berechtigt, für Zwecke der Schulorganisation und der Schulentwicklungsplanung sowie zur Kontrolle und Durchsetzung der Schul- und Berufsschulpflicht eine automatisierte Schülerdatei einzurichten. Darin werden über jede Schülerin und jeden Schüler an den öffentlichen Schulen und den Ersatzschulen des Landes Berlin bis zu 16 Merkmale erfasst. Die einzelnen Merkmale (z. B. Name, Geburtsdatum, Anschrift, Angaben zur Überwachung und Durchsetzung der Schulpflicht, die Befreiung von der Zahlung des Eigenanteils für Lehrmittel) sind im Gesetz[166] in einem Katalog abschließend benannt.

Die Schulen sind zudem verpflichtet, die Daten über die bei ihnen angemeldeten Schülerinnen und Schüler in die automatisierte Schülerdatei einzutragen

165 Vgl. dazu JB 2008, 10.2.2
166 § 64 a Abs. 2 SchulG

und aktuell zu halten[167]. Technisch wird die Schülerdatei von der Senatsverwaltung für Bildung, Wissenschaft und Forschung in einem „Rechenzentrum", das von anderen Einheiten der Senatsverwaltung organisatorisch getrennt ist, im Wege einer **gesetzlichen Auftragsdatenverarbeitung für die Schulen** betrieben. Diese sind – und bleiben – damit als Daten verarbeitende Stelle nach § 4 Abs. 3 Nr. 1 BlnDSG für die von ihnen eingetragenen Datenbestände datenschutzrechtlich verantwortlich. Nachdem uns die Senatsverwaltung für Bildung, Wissenschaft und Forschung über Probleme bei der technischen Implementierung der Datenerfassung durch die Schulen zum Schuljahr 2010/2011 informiert hatte, haben wir empfohlen, die Ersterfassung der Daten für die Schülerdatei als einmaligen Vorgang ebenfalls als Auftragsdatenverarbeitung im Sinne des § 3 BlnDSG (Auftraggeber Schule; Auftragnehmer Senatsverwaltung) auszugestalten.

Die **Datenverarbeitungs- und Zugriffsrechte der Senatsverwaltung** für Bildung, Wissenschaft und Forschung in Bezug auf den personenbezogenen Datenbestand der automatisierten Schülerdatei hat der Gesetzgeber abschließend und restriktiv im SchulG geregelt.[168] Die Senatsverwaltung darf nur auf die personenbezogenen Daten von Schülerinnen und Schülern der (von ihr) zentral verwalteten Schulen zugreifen. Sie darf auf Anfrage im Einzelfall u. a. den Strafverfolgungsbehörden, Polizeibehörden und Jugendämtern mitteilen, auf welche Schule eine Schülerin oder ein Schüler geht.[169] Weitere Daten darf die Senatsverwaltung nur in pseudonymisierter Form (z. B. für die Zwecke der Schulorganisation sowie der Schulentwicklungsplanung) oder sogar nur in nicht-personalisierter aggregierter Form (z. B. für die Befreiung von der Zahlung eines Eigenanteils für Lernmittel) aus der Schülerdatei abrufen.

Durch unsere frühzeitige Einbindung in die Projektplanung und das Gesetzgebungsverfahren zur Einführung der automatisierten Schülerdatei konnten die datenschutzrechtlichen Bedenken, die grundsätzlich mit der Erfassung von personenbezogenen Daten in einer zentralen Datei verbunden sind, weitgehend ausgeräumt werden.

167 § 64 a Abs. 4 SchulG
168 § 64 a Abs. 5 Satz 6 SchulG
169 § 64 a Abs. 8 SchulG

9.2.2 Bitte lächeln! – Weitergabe von Adressdaten an den Schulfotografen

Immer wieder erreichen uns Eingaben, in denen sich die Eltern von Schülerinnen und Schülern über den Umgang mit ihren Adressdaten durch Schulfotografen beschweren. Die externen Dienstleister werden von den Schulen regelmäßig eingeladen, um Klassenfotos oder Bewerbungs- und Portraitfotos von den Schülerinnen und Schülern anzufertigen. Werden die Fotos von den Schülerinnen und Schülern bzw. deren Eltern abgenommen, schließen diese einen zivilrechtlichen Vertrag mit dem Schulfotografen. Die Schule stellt für die Anfertigung der Fotografien lediglich Zeit und Raum zur Verfügung. Dadurch entstehen in der Regel keine vertraglichen Beziehungen mit dem externen Dienstleister. Anders verhält es sich jedoch, wenn dieser für die Schule auch die Schülerausweise im Scheckkartenformat herstellt. Diese enthalten neben dem Lichtbild der Schülerin oder des Schülers auch den Namen, die Anschrift und das Geburtsdatum der Schülerin oder des Schülers. Ein Vater beschwerte sich z. B. darüber, dass diese Daten vom Fotografen auch genutzt wurden, um für nicht bestellte Portraitaufnahmen seines Sohnes eine Rechnung zu erstellen.

Für die Schülerinnen und Schüler des Landes Berlin besteht **keine Pflicht zur Ausstellung eines Schülerausweises.** Es steht ihnen vielmehr frei, für ihre Person von der Schule einen Schülerausweis anfertigen zu lassen. Die Erhebung und Speicherung von personenbezogenen Schülerdaten zum Zweck der Ausstellung von Schülerausweisen ist daher für schulbezogene Aufgaben nicht erforderlich. Sie kann nicht auf § 64 Abs. 1 SchulG gestützt werden und ist zu dem genannten Zweck daher **nur mit Einwilligung der Betroffenen** zulässig. Dem entspricht auch Nr. 1 der Ausführungsvorschriften über Schülerausweise, wonach Schülerinnen und Schüler einen Schülerausweis ausschließlich auf Antrag erhalten. Für Schülerinnen und Schüler der Grundschule ist der Antrag von den Erziehungsberechtigten zu stellen. Es ist somit nicht ausreichend, wenn die Schülerdaten z. B. „auf der Basis einer Absprache mit der Schülergesamtvertretung“ verarbeitet und an den Schulfotografen zur Anfertigung von Schülerausweisen weitergegeben werden. Eine derartige Absprache mit einem Schulgremium kann das Erfordernis einer höchstpersönlichen Einwilligung der Betroffenen in die Verarbeitung ihrer Daten nicht ersetzen.

Die Datenweitergabe zur Erstellung von Schülerausweisen an externe Dritte (z.B. Schulfotografen) erfolgt im Wege der **Auftragsdatenverarbeitung**[170]. Dabei hat die Schule als Auftraggeberin durch vertragliche Regelungen (Weisungen) dafür zu sorgen, dass der Auftragnehmer (Schulfotograf) die Daten nur zu dem beauftragten Zweck nutzt. Nutzt der Auftragnehmer die Daten für einen anderen Zweck, ist dies im Außenverhältnis der Schule (als verantwortlicher Stelle) zuzurechnen.

Bei der Anfertigung von Klassen- und Bewerbungsfotos handelt es sich um keine schulbezogene Aufgabe. Die Übermittlung von Schülerdaten (wie Name, Klasse) durch die Lehrkräfte an den Schulfotografen ist in diesem Zusammenhang daher nur mit der Einwilligung der Betroffenen zulässig. Als grundsätzlich einwilligungsfähig können Schülerinnen und Schüler nach vollendetem 14. Lebensjahr angesehen werden. Bei jüngeren Schülerinnen und Schülern ist die Einwilligung der Erziehungsberechtigten in die Datenübermittlung einzuholen. Nur wenn der externe Dienstleister ein rechtliches Interesse an der Datenübermittlung glaubhaft macht und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der oder des Betroffenen an der Geheimhaltung überwiegt, kann die Datenweitergabe nach § 64 Abs. 5 Nr. 2 SchulG auch ohne Einwilligung erfolgen. Von einem rechtlichen Interesse wäre z. B. dann auszugehen, wenn die Daten dafür benötigt werden, um zivilrechtliche Ansprüche auf Bezahlung von bestellten Fotoaufnahmen geltend zu machen.

Die Erstellung von Schülerausweisen durch einen externen Dienstleister erfolgt im Wege der Auftragsdatenverarbeitung. Die Rechte und Pflichten des Auftragnehmers sind von der Schule verbindlich durch entsprechende vertragliche Regelungen über den Umgang mit personenbezogenen Schülerdaten festzulegen.

170 Nr. 7 der Ausführungsvorschriften

9.2.3 Der „Gang zur Toilette“ – Erfassung von kurzzeitigen Abwesenheiten vom Unterricht

Eine Schülerin beschwerte sich darüber, dass an ihrer Schule der Gang zur Toilette während des Unterrichts von der Lehrkraft notiert werde. Die Namen der Schülerinnen und Schüler, die ihrem „natürlichen Bedürfnis“ nachgehen, würden in Listen erfasst. Die Listen würden in den Klassenbüchern verbleiben und erst vernichtet, wenn sie „voll sind“. Der Sachverhalt wurde uns von der Schulleitung auf Nachfrage bestätigt. Begründet wurde die „Erfassung der Toilettengänge“ damit, dass es in der Vergangenheit mehrfach zu Sachbeschädigungen in den Toilettenräumen gekommen sei.

Durch die Erfassung der Abwesenheitszeiten werden personenbezogene Daten der Schülerinnen und Schüler von den Lehrkräften erhoben und in den Listen gespeichert. Eine derartige Verarbeitung von personenbezogenen Daten ist nach § 6 Abs. 1 Berliner Datenschutzgesetz (BlnDSG) nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat. Nach § 64 Abs. 1 SchulG darf die Schule personenbezogene Daten von Schülerinnen und Schülern verarbeiten, soweit dies zur Erfüllung der ihr durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist.

Die Schülerinnen und Schüler sind nach § 46 Abs. 2 SchulG verpflichtet, regelmäßig am Unterricht und an den sonstigen verbindlichen Schulveranstaltungen aktiv teilzunehmen. Es gehört zu den schulbezogenen Aufgaben, diese Verpflichtung zu kontrollieren und ggf. Verstöße dagegen zu dokumentieren. Dem entspricht § 5 Abs. 1 SchulDatenVO, wonach die Fehlzeiten von Schülerinnen und Schülern (einschließlich Verspätungen und Beurlaubungen) sowie sonstige besondere Vorkommnisse im Klassenbuch festzuhalten sind. Auch das kurzzeitige Verlassen des Unterrichts durch eine Schülerin oder einen Schüler kann daher, vergleichbar einer Verspätung, im Klassenbuch (hier: in einer Liste, die dem Klassenbuch beigelegt ist) erfasst werden.

Allerdings unterliegt diese Datenspeicherung dem **Grundsatz der Erforderlichkeit.** Als Nachweis über die „kurzzeitige Fehlzeit“ ist nur die Speicherung des Namens, Vornamens und der Abwesenheitszeit erforderlich. Die **Erfassung des Abwesenheitsgrundes** (z. B. Toilettengang) ist für den genannten Zweck dagegen nicht erforderlich und damit datenschutzrechtlich **unzulässig**.

Die Vernichtung der Liste (ohne Abwesenheitsgrund) hat zeitnah (jedenfalls nicht erst, wenn sie vollgeschrieben ist), z. B. wöchentlich, zu erfolgen.

Soweit die Erfassung der Schülerdaten damit begründet wurde, dass es mehrfach zu Sachbeschädigungen in den Toilettenräumen gekommen sei, ist anzumerken, dass es sich bei der Aufklärung von Straftaten um keine schulbezogene Aufgabe handelt.

Kurzzeitige Abwesenheiten vom Unterricht dürfen allenfalls ohne Angabe des Grundes (z. B. Toilettenbesuch) erfasst werden. Die Verfolgung und Aufklärung von Straftaten ist originär den Strafverfolgungsbehörden vorbehalten. Eine Verarbeitung von personenbezogenen Schülerdaten zu diesem Zweck kann nicht auf § 64 Abs. 1 SchulG gestützt werden und ist unzulässig.

9.2.4 WebUntis – Anwesenheitserfassung in Schulen

Wir wurden gebeten, eine webbasierte Software zu bewerten, welche die bisherigen papiergebundenen Klassenbücher insbesondere im Zusammenhang mit der Erfassung der Fehlzeiten von Schülerinnen und Schülern ersetzen soll. Auch in anderen Bundesländern gab bzw. gibt es die Bestrebung, diese Software einzusetzen.

Die Software kann entweder als Online-Dienstleistung eingesetzt oder als Offline-Produkt erworben und in den jeweiligen Schulen installiert werden. Bei der Dienstleistungsversion würden die personenbezogenen Daten der Schülerinnen und Schüler sowie der Lehrkräfte auf einem Server des österreichischen Herstellers gespeichert.

Von der Nutzung der Dienstleistungsversion haben wir aus zwei Gründen abgeraten: Erstens kann der ausländische Anbieter von der jeweils verantwortlichen Schule nur schlecht kontrolliert werden. Zudem würde (viele Interessenten vorausgesetzt) eine sehr umfangreiche und sensitive Datensammlung vieler Schulen bei einem Privatunternehmen entstehen. Der zweite Aspekt ist, dass personenbezogene Daten von Schülerinnen und Schülern bisher nur in vom Lehrbetrieb und auch vom Internet abgeschotteten Netzwerken verarbeitet

werden. Insbesondere durch Einsatz der Dienstleistungsversion würde diese Trennung durchbrochen.

Unsere Einschätzung ergab ferner, dass das Offline-Produkt die IT-Sicherheit nicht in ausreichendem Umfang gewährleistet. Insbesondere basiert die Authentifizierung der berechtigten Nutzenden nur auf der Kombination von Nutzername und Passwort. Da die Eintragung von Fehlzeiten auf den schlecht geschützten Computern im Klassenraum erfolgen soll, halten wir diese Art der Authentifizierung für nicht ausreichend. Es muss immer im Auge behalten werden, dass es findige Schülerinnen und Schüler gibt, die in der Lage sind, die Passwörter der Lehrkräfte z. B. mit Keylogger-Tools auszuspähen, um Fehlzeiten zu entfernen.

Grundsätzlich ist gegen die elektronische Verarbeitung sensitiver Schülerdaten nichts einzuwenden, wenn IT-Sicherheitsaspekte wie Netztrennung in der Schule und sichere Authentifizierung beachtet werden. Eine externe Datenverarbeitung sollte nach Möglichkeit vermieden werden.

9.2.5 Forschungsprojekt „Jugendliche als Opfer und Täter von Gewalt“

Das Kriminologische Forschungsinstitut Niedersachsen führte in Zusammenarbeit mit der Senatsverwaltung für Bildung, Wissenschaft und Forschung, der Landeskommission Berlin gegen Gewalt und der Senatsverwaltung für Stadtentwicklung ein Forschungsprojekt zum Thema „Jugendliche als Opfer und Täter von Gewalt“ an Berliner Schulen durch. Dabei sollten ca. 5.000 Berliner Schülerinnen und Schüler der Jahrgangsstufe 9 einen Fragebogen beantworten. Die Studie diente der Erforschung von Gewalt bei Jugendlichen. Entsprechend sensible Fragen wurden den Jugendlichen vorgelegt. So sollten diese zum Beispiel angeben, ob sie bereits Opfer von sexueller Gewalt gewesen seien. Die Fragen bezogen sich allerdings nicht nur auf die Jugendlichen selbst. Es wurde auch nach Details aus dem Familienleben gefragt.

Eine solche Befragung nach persönlichen Verhältnissen kann in das in der Verfassung verankerte Persönlichkeitsrecht der Jugendlichen eingreifen. Dieses Recht gewährleistet, dass der Einzelne selbst über die Preisgabe und Verwendung seiner persönlichen Daten entscheidet. Deshalb kann eine solche Befragung nur freiwillig oder aufgrund eines Gesetzes erfolgen. Nach dem Berliner Schulgesetz dürfen personenbezogene Daten im Rahmen von wissenschaftlichen Untersuchungen in der Regel nur mit Einwilligung der Schülerinnen und Schüler erhoben werden.[171] Bei Kindern und Jugendlichen unter 14 Jahren müssen die Eltern zustimmen.

Uns ist ein Fall bekannt geworden, in dem vergessen worden ist, in einer Klasse solche Einverständniserklärungen einzuholen. Deshalb durften die ausgefüllten Fragebögen nicht für die Studie verwertet werden. Sie wurden unverzüglich vernichtet.

Problematisch war zusätzlich, dass viele Fragen auch die Privatsphäre der Eltern betrafen. Dabei gab es im Einzelnen Fragen nach häuslicher Gewalt, aber auch Fragen nach Religion und Beruf der Eltern sowie nach der Erziehung. Daher war in diesem Fall auch das Persönlichkeitsrecht der Eltern tangiert, sodass auch diese unabhängig vom Alter des Kindes einer Datenerhebung zustimmen mussten. Dieses Recht darf nicht umgangen werden, indem über die Kinder personenbezogene Daten der Eltern erhoben werden. Ohne elterliches Einverständnis durften also auch mit Einwilligung einer über 14 Jahre alten Jugendlichen keine Daten über die persönlichen Verhältnisse der Eltern erhoben werden. Wir haben dazu geraten, in einem solchen Konfliktfall eine Lösung innerhalb der jeweiligen Familie zu suchen. Das Forschungsinstitut hat unsere Empfehlungen aufgegriffen.

Die Teilnahme an Befragungen zu wissenschaftlichen Untersuchungen ist in der Regel freiwillig. Grundsätzlich muss dabei jeder, dessen personenbezogene Daten erhoben werden, selbst zustimmen. Das gilt prinzipiell auch innerhalb einer Familie für jedes einzelne Familienmitglied. Bei Kindern unter 14 Jahren müssen die Erziehungsberechtigten einverstanden sein.

171 § 65 Abs. 3 SchulG

10. Wirtschaft

10.1 Missglückte Einwilligungserklärung bei einer Bank

Aus der Praxis

Eine Berliner Bank hat ihre Kundinnen und Kunden aufgefordert, folgende Einwilligungserklärung zu unterschreiben: „*Ich ermächtige die X-Bank, Transaktionsdaten aus dem Zahlungsverkehr (z. B. Auftraggeber von Lastschriften oder deren Verwendungszweck) zu speichern und diese zu o. g. Zwecken (Werbung für Produkte und Dienstleistungen) auszuwerten. Ausgenommen von dieser Einwilligung sind sensible Daten gem. § 3 Abs. 9 BDSG.*“ Die Bank meinte, ihre Verpflichtungen aus dem Giroverkehr (wie die Information über ungewöhnliche Kontobewegungen) ohne die unterschriebene Einwilligung nicht mehr erfüllen zu können. Die Erklärung diene außerdem dem Schutz der personenbezogenen Daten.

Banken möchten über die von ihnen und ihren Verbundpartnern angebotenen Produkte wie Hypothekenkredite, Fonds und Versicherungen möglichst maßgeschneidert informieren, also Eigenwerbung betreiben. Um festzustellen, welche Produkte den einzelnen Kundinnen und Kunden mit Erfolg angeboten werden können, möchten einige Banken die Transaktionen aus dem Zahlungsverkehr auswerten. Diese enthalten zahllose Daten wie das Einkommen, die Höhe der Verbindlichkeiten, Überweisungen an andere Banken oder Versicherungen und Mietzahlungen. So kann man eine Mieterin oder einen Mieter über günstige Hypothekenzinsen informieren, bei hohem Einkommen Fondssparpläne anbieten oder feststellen, wer unterversichert ist. Die Auswertung der Girokonten erfolgt per Computer nach vorher festgelegten Parametern.

Zur Auswertung der Girokontodaten ist eine Bank nur berechtigt, wenn die Betroffenen wirksam hierin eingewilligt haben. Dies setzt Freiwilligkeit und eine ausreichende Information über den Zweck der Auswertung voraus.[172] Einwilligungserklärungen, die die Bank mit Hilfe von Falschinformationen der Betroffenen erhalten hat, sind unwirksam. Das Missverständnis im Bereich Kundenbetreuung der Bank ist wahrscheinlich durch die fehlerhafte Einwilligungserklärung entstanden. Die Bank lässt sich nicht nur eine Einwilligungserklärung für Datenauswertungen geben, sondern auch für die Speicherung der Girokontodaten, ohne die die Bank ihre Verpflichtungen aus dem Girovertrag nicht erfüllen könnte.

172 § 4a Abs. 1 Satz 1 und 2 BDSG

Die Bank hat den Bereich Kundenbetreuung über die Freiwilligkeit der Einwilligung in Kontoauswertungen informiert. Inzwischen wurde auch die Einwilligung auf die Auswertung von Transaktionsdaten zu Werbezwecken begrenzt.

Banken dürfen die Transaktionen auf den Girokonten ihrer Kundinnen und Kunden nur auswerten, wenn diese wirksam eingewilligt haben.

10.2 Fahrlässiger Umgang mit Bankdaten

Aus der Praxis

Eine Bank wollte einen Kreditnehmer daran erinnern, dass er die fälligen Raten noch nicht bezahlt hat und ihm eine Kreditkündigung droht. Da der Kreditnehmer privat nicht zu erreichen war, rief die Mitarbeiterin in seiner Anwaltskanzlei an. Ein Mitarbeiter des Kreditnehmers meldete sich als dessen Sekretär. Die Bankmitarbeiterin ging irrtümlich davon aus, mit dem Kreditnehmer zu sprechen, und besprach mit ihm die bei dem Kredit aufgetretenen Probleme.

Eine andere Bank hatte mit Partnerbanken vereinbart, bestimmte Kreditanträge an diese weiterzuleiten. Den Antragstellenden wird per E-Mail empfohlen, sich an die jeweilige Partnerbank des jeweiligen Wohnortes zu wenden. In einem Fall wurde das Verfahren dadurch „beschleunigt“, dass die E-Mail-Mitteilung an den Antragsteller nachrichtlich („CC“) an die Partnerbank übermittelt wurde, die sich direkt an den Antragsteller wandte. Die Partnerbank war Arbeitgeberin des Betroffenen, bei der dieser bewusst keinen Kreditantrag gestellt hatte.

Beide Banken sind fahrlässig mit Kundendaten umgegangen, wie sie auch einräumten. Die Erinnerung an fällige Raten sollte grundsätzlich schriftlich erfol-

gen. Eine mündliche Erinnerung sollte auf Ausnahmefälle beschränkt sein (z. B. bei begründeter Vermutung, dass die Betroffenen keine Briefe öffnen). Außerdem ist vor Beginn des Gespräches zu verifizieren, dass man tatsächlich mit der richtigen Person spricht. In der Regel sollte die Bank nur auf Telefonnummern zurückgreifen, die ihr bei Vertragsschluss genannt wurden.

Der Fehler der zweiten Bank kommt – auch außerhalb des Bankensektors – recht häufig vor; immer wieder werden E-Mails ohne größeres Nachdenken nachrichtlich („CC“) an Dritte übermittelt, denen die Information (noch) nicht übermittelt werden darf. Die Information an die Partnerbank hätte erst erfolgen dürfen, nachdem der Kunde sich mit der Weiterleitung seiner Kreditanfrage einverstanden erklärt hat.

Beide Banken haben Vorkehrungen getroffen, dass sich ähnliche Vorfälle nicht wiederholen.

Die Gefahr des fahrlässigen Umgangs mit Bankdaten sollte durch klare interne Regelungen begrenzt werden.

10.3 Aufgedrängte Kommunikation per 1-Cent-Überweisung

Viele Bürgerinnen und Bürger überweisen anlässlich von Katastrophenfällen kleinere Geldbeträge an wohltätige Organisationen, ohne einen weiteren Kontakt mit der Empfängerin der Spende zu beabsichtigen. Sie wollen anonym bleiben. Spendenorganisationen haben allerdings einen neuen Weg der Kontaktaufnahme „entdeckt“: Mit Hilfe der aus der Spende bekannten Kontoverbindungdaten nehmen sie 1-Cent-Überweisungen an die Betroffenen vor. Im Überweisungszweck weisen sie auf die Möglichkeit des Erhalts einer Spendenquittung hin, geben gleichzeitig eine Rückrufnummer bei der Spendenorganisation an und bedanken sich für die getätigte Spende.

Gemeinnützige Organisationen sind regelmäßig auf Spenden angewiesen und daher bestrebt, neue Spenderinnen und Spender zu gewinnen und auf Dauer zu behalten. Gerade nach Katastrophenfällen gibt es viele spontane Spenden. Die Spendenorganisationen sind daran interessiert, die Adressen der Betroffenen zu erfahren, um sich bei ihnen zu bedanken und sie nach gewisser Zeit erneut um eine Spende zu bitten.

Kontoverbindungsdaten sind für finanzielle Transaktionen, nicht aber als Ersatz für die üblichen Kommunikationswege gedacht. Spendenorganisationen dürfen mit Hilfe von 1-Cent-Überweisungen keine Hinweise auf Spendenquittungen geben, da diese Hinweise nicht erforderlich sind.[173] Es gibt zudem keine gesetzliche Verpflichtung der Spendenorganisationen, eine Spendenquittung zu erteilen. Außerdem können sie über die Möglichkeit des Erhalts von Spendenquittungen allgemein informieren, z. B. über das Internet oder auf Werbeflyern. Für Spenden im Katastrophenfall reicht bei anerkannten Spendenempfängerinnen außerdem ein Bareinzahlungsbeleg oder eine Buchungsbestätigung als einfacher Spendennachweis gegenüber dem Finanzamt aus. Selbst wenn die 1-Cent-Überweisung als Werbung eingestuft würde, wäre diese Praxis unzulässig. Denn Kontodaten sind nicht vom sog. Listenprivileg erfasst[174] und dürfen daher nicht zu Werbezwecken genutzt werden.

Verschiedene Spendenorganisationen, die dieses Verfahren nutzten, haben auf unsere Aufforderung hin die Praxis der 1-Cent-Überweisungen eingestellt.

Das von manchen Spendenorganisationen praktizierte Verfahren der 1-Cent-Überweisungen, bei dem auf die Möglichkeit von Spendenquittungen hingewiesen und ein Dank für die Spende ausgesprochen wird, ist rechtswidrig.

173 § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG
174 § 28 Abs. 3 Satz 2 BDSG; vgl. dazu 2.2

10.4 Auftragsdatenverarbeitung durch Heimarbeit

Aus Kostengründen traf eine außerhalb Berlins ansässige Versicherung die Entscheidung, telefonische Anfragen von Kundinnen und Kunden durch externe Dienstleister bearbeiten zu lassen. Das beauftragte Berliner Unternehmen gab diesen Auftrag an einen Dritten (ebenfalls ein Berliner Unternehmen) weiter. Dieser wiederum beauftragte ein auf Telefondienstleistungen spezialisiertes Unternehmen (Unterunterauftragnehmer). Dieses Unternehmen führte die Beratungen aber ebenfalls nicht selbst durch, sondern beauftragte selbstständige Beraterinnen und Berater, die von zu Hause aus tätig wurden. Hierzu hatten sie per heimischem Computer Zugriff auf die Versichertendaten. Sie hatten sich auf Ausschreibungen im Internet beworben. Dabei mussten sie insbesondere nachweisen, dass sie beim Finanz- und Gewerbeamt als Selbstständige geführt werden.

Das „Outsourcen" des Telefonservice stellt in der Regel eine Auftragsdatenverarbeitung dar, die möglich ist, soweit sie nicht zu einer Verletzung von Privatgeheimnissen[175] führt. Allerdings muss der Auftraggeber mit den Auftragnehmern Verträge abschließen, die ausreichende technische und organisatorische Maßnahmen der Auftragnehmer und die Kontrollrechte des Auftraggebers sicherstellen.[176] Vorliegend gab es zwar zwischen den verschiedenen Beteiligten Verträge. Diese betrafen aber nicht bzw. kaum Fragen des Datenschutzrechts und der Datensicherheit. Eine Kontrolle der selbstständigen Beraterinnen und Berater war nicht vorgesehen. Die vom Gesetz geforderte sorgfältige Auswahl der Auftragnehmer fand nicht statt. Betroffene, die glaubten, von ihrer Versicherung beraten zu werden, wurden in Wirklichkeit von selbstständigen Heimarbeiterinnen oder Heimarbeitern beraten, möglicherweise aber auch von deren Angehörigen oder sonstigen Dritten. Da die Selbstständigen ihre private Computerinfrastruktur nutzten, war schon aus diesem Grunde eine ausreichende Datensicherheit nicht gegeben.

Nach Bekanntwerden des „Outsourcingmodells" hat die Versicherung die Zusammenarbeit mit den Auftragnehmern gekündigt. Gegen die Berliner Unternehmen haben wir ein Ordnungswidrigkeitenverfahren eingeleitet.

175 § 203 StGB
176 § 11 Abs. 2 BDSG

Auftragsdatenverarbeitung erfordert die sorgfältige Auswahl des Auftragnehmers, seine Kontrolle und die Erteilung schriftlicher Weisungen. Die Gefahr von Kontrollverlust und Missbrauch steigt bei Auftragsdatenverarbeitungsketten deutlich.

10.5 Das neugierige Fitnessstudio

Ein Bürger wollte sich in einem Fitnessstudio über dessen Angebot und die Vertragsbedingungen für eine Mitgliedschaft informieren. Vor dem Beratungsgespräch erhielt der Interessent einen Fragebogen, den er ausfüllen sollte. Als er dieses ablehnte, verweigerte man ihm das Beratungsgespräch. In dem umfangreichen Fragebogen wurden u. a. folgende Daten erhoben: Name, Vorname, Adresse, Geburtsdatum, Telefonnummer, E-Mail, Anzahl der Kinder. Daneben mussten Fragen zu etwaigen Verletzungen und zur momentanen körperlichen Verfassung beantwortet werden, auch weshalb man sich in dieser Verfassung befindet. Außerdem war anzugeben, wie lange man darüber nachgedacht habe, mit dem Training zu beginnen und welche Umstände (Familie, Finanzen o. Ä.) dazu geführt haben, dass man nicht schon früher mit dem Training begonnen hat.

Vor einem Beratungsgespräch in einem Fitnessstudio dürfen nur Daten abgefragt werden, die erforderlich sind, um das Beratungsgespräch durchzuführen. Dies sind insbesondere Informationen über die Leistungen, die die Interessentin oder der Interessent von dem zukünftigen Fitnessstudio erwartet. Die abgefragten Grund- und Kontaktdaten waren demgegenüber nicht erforderlich und dienten dazu, die Interessierten bei Nichteintritt zu bewerben. Insbesondere war es nicht gestattet, sensitive Daten zu Verletzungen oder zur körperlichen Verfassung abzufragen. Durch unsere Intervention konnten wir erreichen, dass der Fragebogen deutlich „abgespeckt wurde". Außerdem werden die Betroffenen inzwischen darauf hingewiesen, dass das Ausfüllen des Fragebogens freiwillig erfolgt, also auch einzelne Fragen unbeantwortet bleiben können.

Fitnessstudios dürfen von Interessentinnen und Interessenten zur Vorbereitung eines Beratungsgesprächs nur im begrenzten Umfang und auf freiwilliger Basis Daten erheben.

10.6 Praxis der Sanktionsstelle

Wir haben erneut zahlreiche Bußgeldverfahren eingeleitet. Die überwiegende Anzahl dieser Verfahren betraf Fälle, in denen Unternehmen uns (meistens fahrlässig) keine Auskunft erteilt haben. Wir sind auf diese Auskünfte angewiesen, weil wir ansonsten die Eingaben von Bürgerinnen und Bürgern nicht prüfen können.

In 22 Fällen haben wir einen Bußgeldbescheid erlassen oder eine Verwarnung ausgesprochen und dabei Buß- und Verwarnungsgelder von insgesamt 35.120 Euro festgesetzt.

Mit der Novellierung des BDSG 2009 hat der Gesetzgeber zahlreiche neue Bußgeldtatbestände geschaffen, die in einigen Fällen vorlagen. In einem Fall nutzte ein Unternehmen trotz Widerspruchs des Betroffenen dessen Anschrift für seine Werbemaßnahmen. Die Nutzung von Daten der Betroffenen zu Werbezwecken ist bei einem Widerspruch jedoch unzulässig. Wir haben deshalb für diese rechtswidrige Nutzung ein Bußgeld verhängt.[177] Nach altem Recht konnte eine rechtswidrige Nutzung von Daten in keinem Fall geahndet werden. Die Unternehmen sollen durch diese neue Sanktionsmöglichkeit dazu angehalten werden, mit Widersprüchen der Betroffenen sorgfältig umzugehen und diese zu beachten.

In zwei anderen Fällen lag kein ordnungsgemäßer Auftragsdatenverarbeitungsvertrag vor. Solche Verträge werden geschlossen, wenn die beauftragte Stelle nur eine Hilfs- und Unterstützungsfunktion hat und in völliger Abhängigkeit von den Vorgaben des Auftraggebers agiert, ähnlich einer ausgelagerten Abteilung. Der Gesetzgeber hat nunmehr detailliert geregelt, welche Mindestbestandteile ein solcher Vertrag enthalten muss.[178] Diese Anforderungen waren in den zwei Fällen nicht bzw. nicht vollständig erfüllt, sodass wir ebenfalls ein Bußgeld festgesetzt haben. Die Festsetzung von Bußgeldern in solchen Fällen[179] trägt dazu bei, die gesetzlichen Rahmenbedingungen der Auftragsdatenverarbeitung besser durchsetzen zu können.

177 § 43 Abs. 2 Nr. 5b BDSG

Unternehmen, die gegen Datenschutzvorschriften verstoßen, müssen mit Bußgeldverfahren rechnen. Werbewidersprüche von Betroffenen sind zu beachten. Die Unternehmen haben entsprechende organisatorische Maßnahmen zu ergreifen. In Auftragsdatenverarbeitungsverträgen sind die gesetzlichen Mindestanforderungen zu regeln. Unternehmen, die sich solcher Auftragsdatenverarbeiter bedienen, sollten bestehende Verträge überprüfen.

10.7 Technische Umsetzung der EU-Dienstleistungsrichtlinie

Die EU-Dienstleistungsrichtlinie sieht vor, dass jeder Mitgliedstaat und jedes Bundesland einen Einheitlichen Ansprechpartner (kurz: EA) als Schnittstelle zu den Anmelde- und Genehmigungsbehörden insbesondere ausländischen Dienstleistern zur Verfügung stellen, die sich in dem jeweiligen Land niederlassen wollen[180].

In Berlin wurde zur Unterstützung des EA ein **Web-Portal** realisiert, über das sich die Dienstleister einerseits über die notwendigen Schritte zur Anmeldung eines Vorhabens informieren und andererseits über ein Dialogsystem alle notwendigen Anträge stellen und die notwendigen Unterlagen einreichen können. Das Portal bietet zudem Schnittstellen zu den jeweiligen Fachbehörden und ermöglicht dem EA so die effiziente, idealerweise durchgehend elektronische Abwicklung eines Antrages einschließlich der Überwachung von Fristen,

178 § 11 Abs. 2 Satz 2 BDSG
179 § 43 Abs. 1 Nr. 2b BDSG
180 Zur rechtlichen Umsetzung der Dienstleistungsrichtlinie vgl. JB 2008, 11.5; JB 2009, 10.9

des Einzuges der Gebühren und der Übersendung der Bescheide der Fachbehörden. Neben der Begleitung der für das Vorhaben notwendigen Gesetzesänderungen haben wir die technische Realisierung des Portals aus Datenschutz- und IT-Sicherheitssicht geprüft.

Nimmt ein Dienstleister die Unterstützung des EA bei der Bearbeitung eines Antrages in Anspruch, so ist unvermeidlich, dass Mitarbeitende des EA aufgrund der gesetzlich vorgesehen formalen Prüfung der eingereichten Unterlagen sowie der Überwachung des Verfahrensablaufes personenbezogene Daten der Antragstellenden erhalten und nahezu alle antragsbezogenen Unterlagen im **Dokumentenmanagementsystem** des EA zusätzlich zu den Akten in den Fachbehörden gespeichert werden müssen. Allerdings wird der Zugriff zu diesen Informationen durch ein strenges **Rechtemanagement** eng begrenzt. Bei dem EA sowie in den jeweiligen Fachbehörden hat nur die bzw. der Bearbeitende des Falles direkten Zugriff auf die Falldaten. Zusätzlich haben ausgewählte Mitarbeitende das Recht, Fälle anderen Beschäftigten zuzuteilen.

Die jeweilige Fachbehörde hat nur Zugriff auf die für sie relevanten Dokumente. In der Regel müssen für die Anmeldung einer Dienstleistung mehrere Fachbehörden einbezogen werden. Der Dienstleister kann die notwendigen Unterlagen elektronisch einreichen, ggf. signiert mit einer qualifizierten digitalen Signatur. Alternativ können auch handschriftlich unterschriebene Anträge oder beglaubigte Kopien von Dokumenten eingereicht werden. Bescheide der Fachbehörden kann der Dienstleister aus seinem Postfach im Portal sicher herunterladen. Die Kommunikation erfolgt dabei zum **Schutz der Vertraulichkeit** verschlüsselt.

Mittelfristig sollten jedoch Dienstleister und Beschäftigte mittels besserer Mechanismen bei der Anmeldung zum System authentifiziert werden. Derzeit wird die Kombination von Nutzernamen und Passwort verwendet, um die Einstiegshürden für die Dienstleister möglichst niedrig zu halten. Die Anmeldung der Beschäftigten ist zur Sicherheit nur innerhalb der Infrastruktur des Landesnetzes möglich. Vorgesehen ist zukünftig die **Nutzung des neuen Personalausweises**[181] für Registrierung und Anmeldung.

181 Vgl. 2.4

Als datensparsame Alternative bietet sich das Informationsangebot des EA an. Ebenfalls über ein Dialogsystem werden die relevanten Daten des Vorhabens des Dienstleisters erfragt und im Ergebnis ohne Erhebung eines Personenbezuges ein Dokument mit Hinweisen zu den nötigen Genehmigungen samt Adressen und einzureichenden Formularen der jeweiligen Fachbehörden ausgegeben.

Das Web-Portal des EA in Berlin bietet ein ausreichendes Maß an IT-Sicherheit und Datenschutz. Der Dienstleister sollte bei der Nutzung des Portals auf die Sicherheit seines eigenen Rechners sowie auf ein sicheres Passwort achten. Wenn er es vorzieht, kann der Dienstleister das Informationsangebot des EA auch wahrnehmen, ohne sich zu identifizieren, und anschließend die Anträge direkt bei den Fachbehörden stellen.

11. Europäischer und internationaler Datenschutz

11.1 Europäische Union

Mit dem Ende 2009 in Kraft getretenen Vertrag von Lissabon haben sich die rechtlichen Rahmenbedingungen für den Datenschutz in der Europäischen Union grundlegend geändert. Die seitdem geltende Charta der Grundrechte der Europäischen Union enthält eine verbindliche Regelung zum Schutz personenbezogener Daten.[182] Der Vertrag über die Arbeitsweise der Europäischen Union verpflichtet dazu, einheitliche Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowohl auf EU- als auch auf mitgliedstaatlicher Ebene zu erlassen.[183] Dementsprechend hat die Europäische Kommission eine Überarbeitung der Europäischen Datenschutzrichtlinie 95/46/EG angekündigt, auch weil die technologische Entwicklung und die Globalisierung den Datenschutz vor neue Herausforderungen stellen.

Ende des Jahres hat die Europäische Kommission eine **neue Strategie zur Stärkung des EU-Datenschutzrechts** vorgestellt.[184] Als Kernziele nennt sie die Stärkung der Rechte des Einzelnen, die bessere Harmonisierung des Datenschutzes in der Wirtschaft, die Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit der Polizei- und Strafjustizbehörden, die Gewährleistung eines hohen Schutzniveaus bei außerhalb der EU übermittelten Daten und die wirksamere Durchsetzung der Vorschriften. Im Rahmen der öffentlichen Konsultation haben die Datenschutzbeauftragten des Bundes und der Länder zum Gesamtkonzept Stellung genommen.[185] Insbesondere begrüßen sie den Grundansatz, dass vor dem Hintergrund des Wegfalls der Säulenstruktur der Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in

182 Art. 8
183 Art. 16 AEUV
184 Mitteilung der Europäischen Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4. November 2010, KOM(2010) 609, endg., BR-Drs 707/10
185 Der Konsultationsbeitrag ist abrufbar unter www.bfdi.bund.de.

den Anwendungsbereich des neuen Rechtsrahmens einbezogen werden soll.[186] Anzustreben ist ein möglichst einheitliches Datenschutzniveau in Europa. Der neue europäische Rechtsrahmen darf andererseits nicht zu einer Absenkung des Datenschutzes in Deutschland führen.

Im August ist das neue **EU-US-Abkommen zur Übermittlung von Zahlungsverkehrsdaten**[187] in die USA in Kraft getreten. Allerdings entspricht es auch in der Neufassung nicht den durch die EU-Grundrechtecharta und die Europäische Datenschutzrichtlinie vorgegebenen Standards. Weder der Umfang der Datenübermittlung noch die Kriterien für den Datenzugriff sind hinreichend bestimmt, und die vorgesehene Speicherdauer von fünf Jahren ist unverhältnismäßig lang. Grotesk ist, dass ausgerechnet Europol den Umfang der in die USA übermittelten Daten überwachen soll – eine Behörde, die letztlich von den US-Diensten mit den aus dem Datenbestand gewonnenen Erkenntnissen versorgt wird. Eine unabhängige Instanz zur Kontrolle des Datenschutzes ist Europol deshalb nicht. Immerhin haben EU-Bürger nun ein Recht auf Auskunft, Berichtigung, Löschung und Sperrung.[188] Anträge von Betroffenen sind an ihre Datenschutzbehörde in der Europäischen Union bzw. ihre nationale Aufsichtsbehörde zu richten, die sie an den Datenschutzbeauftragten des US-Finanzministeriums weiterleitet. Die an uns gerichteten Anträge leiten wir, wie die Kollegen in den anderen Bundesländern, an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit weiter, damit eine einheitliche Handhabung gewährleistet ist.

Neue Entwicklungen gibt es zur **Übermittlung von EU-Flugpassagierdaten**[189] **in Drittländer.** Das Europäische Parlament hat die Europäische Kommission im Mai aufgefordert[190], spätestens bis Mitte Juli einen kohärenten Ansatz in Bezug auf die Nutzung von Fluggastdatensätzen für Strafverfolgungs- und Sicherheitszwecke und ein auf einheitlichen Grundsätzen beruhendes Modell für ein solches Abkommen mit Drittstaaten vorzulegen. Dieser

186 Vgl. bereits JB 2009, 11.1 (S. 158); JB 2008, 12.1
187 Terrorist Finance Tracking Program (TFTP) II-Abkommen, besser bekannt als SWIFT-Abkommen; hierzu zuletzt JB 2009, 11.1
188 Art. 15, 16 des Abkommens
189 Sog. Passenger Name Records (PNR)
190 Entschließung des Europäischen Parlaments vom 5. Mai 2010

Aufforderung ist die Kommission im September nachgekommen.[191] Das Paket mit Vorschlägen über den Austausch von PNR-Daten mit Drittländern enthält eine allgemeine EU-Außenstrategie zum Thema Fluggastdaten sowie Empfehlungen für Verhandlungsrichtlinien für neue PNR-Abkommen mit den USA, Australien und Kanada.[192]

Im engen Zusammenhang mit den Beratungen zu den PNR-Abkommen steht auch das geplante Übereinkommen zwischen der EU und den USA über den Schutz personenbezogener Daten und **Informationsaustausch zu Strafverfolgungszwecken**.[193] Die beabsichtigte Vereinbarung soll keine eigenen Rechtsgrundlagen für Datenübermittlungen enthalten, sondern als Rahmenübereinkunft Datenschutzstandards vorgeben, die bei der strafrechtlichen Zusammenarbeit, z. B. bei der Übermittlung von Zahlungsverkehrs- oder Fluggastdaten, eingehalten werden. Wesentlich wäre, anlasslose Übermittlungen ganzer Datenpakete und die Verwendung der Daten zu anderen Zwecken als der strafrechtlichen Zusammenarbeit auszuschließen.[194]

Die Europäische Kommission hat erneut[195] eine Entscheidung zu **Standardvertragsklauseln** für die Übermittlung personenbezogener Daten in Drittländer getroffen[196] und damit auf neue Anforderungen aus der Wirtschaft reagiert. Die Klauseln sollen den Datenschutz auch dann sicherstellen, wenn Datenverarbeiter außerhalb der EU Aufgaben ihrerseits von Subunternehmern erledigen lassen. Dies ist nur mit Zustimmung des Unternehmens in der EU möglich, das die Daten ursprünglich erhoben hat. Die neuen Standardvertragsklauseln gelten seit Mai und ersetzen die bislang für die Auftragsdatenverarbeitung geltenden vom Dezember 2001.

Die **Art.29-Datenschutzgruppe,** in der wir die Bundesländer vertreten, hat wieder mehrere Papiere verabschiedet. Sie befasste sich speziell mit den

191 Mitteilung der Kommission über das Sektor übergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer, KOM(2010) 492, endg.
192 Zur Entwicklung der Thematik vgl. JB 2003, 4.7.1 (a. E.); JB 2007, 10.1
193 Sog. Datenschutz-Rahmenabkommen
194 So auch die Bundesratsinitiative Hamburgs, BR-Drs 741/10
195 Vgl. zuletzt JB 2004, 4.7.1 (S. 121)
196 Beschluss 2010/87/EU vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, ABl. L 39 vom 12. Februar 2010, S. 5, vgl. Dokumentenband 2010, S. 70

Begriffen “für die Verarbeitung Verantwortlicher“ und „ Auftragsverarbeiter“[197], mit der Werbung auf Basis von Behavioural Targeting[198] und mit einem Vorschlag für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen.[199] Auch hat sie FAQs zu den neuen für die Auftragsdatenverarbeitung geltenden Standardvertragsklauseln[200] erarbeitet.[201] Schließlich hat sie sich mit der Mitteilung der Europäischen Kommission über das Sektor übergreifende Konzept für die Übermittlung von Fluggastdatensätzen an Drittländer befasst[202] und das einheitliche Vorgehen in den Verhandlungen mit verschiedenen Drittländern als Schritt in die richtige Richtung begrüßt.[203] Ein Papier gibt darüber hinaus Hilfestellung für die Bestimmung des anwendbaren Rechts bei grenzüberschreitender Datenverarbeitung.[204]

11.2 AG „Internationaler Datenverkehr“

Auf Vorschlag der unter unserem Vorsitz tagenden AG „Internationaler Datenverkehr“ hat der Düsseldorfer Kreis einen Beschluss gefasst, mit dem darauf hingewiesen wird, dass sich Unternehmen bei Datenübermittlungen in die USA nicht mehr allein auf die Behauptung einer **Safe Harbor-Zertifizierung** des Datenimporteurs verlassen können und sich diese nachweisen lassen müssen.[205] Es hatte begründete Zweifel gegeben, dass die Safe Harbor-Grundsätze in der Regel von den Mitgliedsunternehmen nicht eingehalten werden. Auch wurden Vollzugsdefizite, die mangelnde Sanktionierung von Verstößen,

197 Stellungnahme 1/2010 vom 16. Februar 2010 (WP 169)
198 Stellungnahme 2/2010 vom 22. Juni 2010 (WP 171), vgl. Dokumentenband 2010, S. 92
199 Stellungnahme 5/2010 vom 13. Juli 2010 (WP 175)
200 Vgl. Fn. 196
201 Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG vom 12. Juli 2010 (WP 176), vgl. Dokumentenband 2010, S. 130
202 Vgl. Fn. 191
203 Stellungnahme 7/2010 vom 12. November 2010 (WP 178)
204 Stellungnahme 8/2010 vom 16. Dezember 2010 (WP 179)
205 Beschluss vom 28./29. April 2010 i. d. F. vom 23. August 2010: Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, vgl. Dokumentenband 2010, S. 22

die unwahre Behauptung mehrerer Unternehmen, den Grundsätzen beigetreten zu sein, sowie die Tatsache kritisiert, dass die vom US-Handelsministerium geführte Liste[206] Unternehmen enthält, die nicht mehr Mitglied des Programms sind.[207]

Daneben hat sich die AG mit komplizierten E**inzelfragen zur internationalen Auftragsdatenverarbeitung** befasst. Sie hat die von der Wirtschaft häufig gestellte Frage, ob die neuen Standardvertragsklauseln zur Auftragsdatenverarbeitung[208] auch für die innereuropäische Auftragsdatenverarbeitung verwendet werden können, verneint, denn alleiniger Maßstab hierfür ist § 11 Abs. 2 BDSG. Deshalb kann der Standardvertrag nur mit Änderungen in der Terminologie und bei den einzelnen Klauseln für die innereuropäische Auftragsdatenverarbeitung genutzt, jedoch keinesfalls als solcher bezeichnet werden.

Auch wurde erörtert, ob die für die Einhaltung des § 11 BDSG erforderliche Präzisierung des neuen Standardvertrags eine Genehmigungspflicht nach § 4c Abs. 2 BDSG auslöst. Das wurde ebenfalls verneint: Wird ein Standardvertrag zur Auftragsverarbeitung geschlossen, so sind die Anforderungen des § 11 BDSG dadurch bereits teilweise erfüllt. Die erforderliche Präzisierung kann in den Anlagen zum Standardvertrag realisiert werden, die immer die konkreten Bedingungen des jeweiligen Datentransfers widerspiegeln und notwendigerweise variieren. Anpassungen in diesem Bereich lösen daher grundsätzlich keine Genehmigungspflicht aus, solange dort nicht dem Vertrag selbst widersprechende Regelungen getroffen werden. Auch Präzisierungen durch zusätzliche geschäftliche Klauseln oder in einem separaten Dienstleistungsvertrag mit zugehöriger Leistungsbeschreibung, auf den Bezug genommen wird, sind möglich und lösen keine Genehmigungspflicht aus; denn sie betreffen zum einen die sog. 1. Stufe, und zum anderen geht aus den Standardverträgen selbst hervor, dass ihre Regelungen nicht so konkret sind, dass sie die Pflichten des Auftragnehmers abschließend beinhalten. Zudem ist die Unterbeauftragung nach dem neuen Standardvertrag genehmigungsfrei. Es wäre sinnwidrig, wenn der Vertrag wegen der Anpassung an § 11 BDSG genehmigungspflichtig würde.

206 www.export.gov/safeharbor/
207 Vgl. Ch. Connolly, Galexia Australia: The US Safe Harbor – Fact or Fiction?, 2008
208 Vgl. Fn. 196

11.3 Internationale Datenschutzstandards

Internationale Datenschutzstandards können Verarbeiter von personenbezogenen Daten darin unterstützen, datenschutzgerecht zu handeln. Wir trugen zur Formulierung eines Datenschutzrahmenstandards der Internationalen Standardisierungsorganisation ISO bei und forderten auf der ersten Internationalen Datenschutz-Konferenz der ISO die Erarbeitung von Standards zum Datenschutzmanagement.

Schon 2004 war im Rahmen der ISO der Versuch unternommen worden, einen nicht-technischen Rahmenstandard für den Datenschutz zu formulieren. Sowohl die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group")[209] als auch die 26. Internationale Datenschutzkonferenz[210] kritisierten seinerzeit, dass bei diesem Versuch wesentliche Grundsätze des Datenschutzrechts zu wenig berücksichtigt worden seien, und boten der ISO eine Zusammenarbeit an. Dieses Angebot wurde angenommen; die Zusammenarbeit, in die auch die Art. 29-Gruppe einbezogen wurde, beginnt jetzt Früchte zu tragen.

Im Berichtsjahr nahm der Datenschutzrahmenstandard 29100 der ISO eine endgültige Form an. Es werden eine einheitliche Terminologie für die Beschreibung der Datenverarbeitung eingeführt und die wichtigsten Datenschutzprinzipien niedergelegt, die sich auch in der deutschen und europäischen Gesetzgebung widerspiegeln.

Wir begleiteten diesen Prozess durch die Beteiligung an einem Gremium des Deutschen Instituts für Normung, das für den deutschen Beitrag zur Standardisierung auf den Gebieten des Datenschutzes und des Identitätsmanagements verantwortlich ist. Wie in den vergangenen Jahren waren wir maßgeblich an der Erarbeitung der Kommentare zu den Entwürfen des Datenschutzrahmenstandards beteiligt.

209 Arbeitspapier zu einem zukünftigen ISO-Datenschutzstandard, vgl. Dokumentenband 2004, S. 73
210 Resolution zum Entwurf eines ISO-Rahmenstandards zum Datenschutz, vgl. Dokumentenband 2004, S. 67 ff.

Im Oktober fand die erste Internationale Datenschutz-Konferenz der ISO statt, während der internationale Experten erörterten, wie der Datenschutz im Zuge der Standardisierung technischer Verfahren unterstützt werden kann und welche Erfolge bereits jetzt vorzuweisen sind. Wir legten dar, welchen Zwecken internationale Datenschutzstandards dienen können und auf welchen Gebieten derartige Standards erforderlich sind.

Transparenz

International agierende Konzerne, die ihr Personal zentral verwalten und Produkte und Dienstleistungen über das Internet einer internationalen Kundschaft anbieten, und Unternehmen, die ihre Geschäftsprozesse über Ländergrenzen hinweg eng miteinander verzahnen, müssen ihre Datenverarbeitung transparent gestalten. Sie müssen die Einhaltung der jeweiligen nationalen Gesetze gewährleisten und die ihrer Geschäftspartner einschätzen. Betroffene (Kundschaft und Beschäftigte) müssen in die Lage versetzt werden zu verstehen, was mit ihren Daten geschieht. Datenschutzaufsichtsbehörden und andere Aufsichtsbehörden[211] müssen die Einhaltung nationaler Gesetze und internationaler Abkommen beurteilen.

Standards können einen Rahmen und eine universelle Terminologie anbieten, mit denen sich die Ziele und Prozesse des Datenschutzes beschreiben lassen und Transparenz hergestellt wird. Unternehmen und Behörden können mit ihrer Hilfe die Datenschutzprinzipien beschreiben, zu deren Einhaltung sie sich verpflichten, die Methoden darstellen, die sie nutzen, um die Daten zu sichern, und auch die Prozesse schildern, mit denen sie die Einhaltung der gesetzlichen Vorgaben garantieren. Dies ist insbesondere dann von Bedeutung, wenn die Parteien sehr unterschiedlichen Rechtskreisen angehören. Wo Rechtsnormen zum Datenschutz existieren, können sie von Standards weder unterschritten noch ersetzt werden. Standards können aber die einheitliche Durchsetzung von Rechtsnormen unterstützen.

211 Etwa die Federal Trade Commission in den USA

Datenschutzmanagement

Die Standardisierung des Managements der Informationssicherheit ist eine Erfolgsgeschichte, die erheblich zu einem höheren Sicherheitsniveau der Standardanwender geführt hat. Datenschutzmanagement kann und sollte diesem Beispiel folgen. Datenschutzmanagement-Systeme sollen einen Prozess zur Verfügung stellen, in dem eine systematische Analyse der Verarbeitung von personenbezogenen Daten vollzogen werden kann. Hierbei müssen die verschiedenen Risiken, denen die Privatsphäre der Betroffenen durch Bedrohungen innerhalb und außerhalb der jeweiligen Organisation ausgesetzt ist, und die Folgen, die bei unrechtmäßiger Kenntniserlangung eintreten, abgeschätzt werden. Aus dieser Bedrohungslage kann dann ein umfassendes Geflecht von Maßnahmen entwickelt werden, die den Schutz der Betroffenen in angemessener Weise gewährleisten. Schließlich muss es ein Datenschutzmanagement-System erlauben, ein Datenschutzkonzept nicht nur einmalig zu entwickeln, sondern auch konstant fortzuschreiben. Internationale Standards haben das Potenzial, eine erstrangige Leitlinie für die Errichtung derartiger Datenschutzmanagement-Systeme zu werden. Sie können die Wege aufzeigen, mit denen die angemessenen Datenschutzmaßnahmen ausgewählt und die Einhaltung der festgelegten Datenschutzprinzipien überprüft werden.

Datenschutzwerkzeuge

Datenschutz erfordert Informationssicherheit. Ohne technische Gewährleistung, dass Dritte nicht unberechtigt die verarbeiteten personenbezogenen Daten zur Kenntnis nehmen können, ist Datenschutz nicht denkbar. Technologie kann jedoch mehr, als nur die Dämme zu errichten, innerhalb derer Daten geschützt fließen; sie kann den Strom selbst formen. Verschiedene „Privacy Enhancing Technologies“ (spezifische Techniken der Minimierung der Datenoffenbarung) können dazu benutzt werden, zeitweilig oder permanent die Verknüpfung von Daten zu den Personen, auf die sie sich beziehen, zu verbergen, ohne dass die Verarbeitung der Daten eingeschränkt wird. Zu diesen Techniken gehören die Pseudonymisierung, sichere Mehrparteienberechnungen, datenschutzfreundliche Datenaggregation und informationsarme Identifikationsverfahren. Einige dieser Verfahren sind bereits standardisiert. Andere sollten folgen.

Bereichsspezifische Standards für gestalteten Datenschutz (Privacy by design)

Spezifische Datenschutzrisiken bestehen insbesondere in der Telekommunikationsbranche, der Gesundheitsversorgung und dem Finanzdienstleistungssektor. So hat das für die Standardisierung der Verarbeitung von Gesundheitsdaten zuständige Komitee der ISO bereits eine Reihe von Standards verabschiedet, die direkten Einfluss auf den Datenschutz bei den Erbringern von Gesundheitsdienstleistungen haben. Aufstrebende Sektoren, die besonderer Beachtung bedürfen, sind z. B. Systeme für die Lenkung des Fahrzeugverkehrs, intelligente Stromnetze und Internetdienste mit Zugriff auf den Aufenthaltsort der Nutzenden. Gleichfalls entwickelt sich die Anwendung von Technologien rasant, die besondere Datenschutzrisiken bergen: die Geschäftsanalyse großer Mengen unstrukturierter Daten in Datenbanken (Data Warehousing), Videoüberwachung und biometrisches Identitätsmanagement, um nur einige wenige mit bereits weiter Verbreitung zu nennen. Die Anwendung dieser Techniken wird in hohem Maße durch internationale Standards bestimmt. Ein datenschutzfreundlicher Ansatz für ihre Gestaltung sollte sich also bereits in diesen Standards finden.

Internationale Standards können Methoden und Werkzeuge bieten, um in der internationalen Datenverarbeitung Transparenz zu erzielen, den Verarbeitern ein effektives Management des Datenschutzes zu ermöglichen, einzelne Verarbeitungsschritte datenarm auszugestalten und den besonderen Risiken bestimmter Verarbeitungsformen entgegenzuwirken.

12. Datenschutzmanagement

12.1 Stiftung Datenschutz – ein Zwischenstand

Unabhängig von etwaigen gesetzgeberischen Tätigkeiten[212] plant die Bundesregierung eine interessante Neuerung: Im Koalitionsvertrag (2009 – 2013) vereinbarten die Regierungsparteien die Errichtung einer „Stiftung Datenschutz“ mit dem Ziel, den Datenschutz zu stärken. Das wird von den Datenschutzbeauftragten des Bundes und der Länder nachdrücklich unterstützt.[213] Datenschutz kann in der modernen Informationsgesellschaft nicht mehr allein mit Verboten und anderen Mitteln des Ordnungsrechts durchgesetzt werden.

Laut Koalitionsvertrag soll die Stiftung den Auftrag haben, Produkte und Dienstleistungen auf **Datenschutzfreundlichkeit** zu prüfen, **Bildung** im Bereich des Datenschutzes zu stärken, den **Selbstdatenschutz durch Aufklärung** zu verbessern und ein **Datenschutzaudit** zu entwickeln. Ein konkretes Konzept zur Ausgestaltung der Stiftung liegt bislang nicht vor.[214] Viele Fragen sind offen, z. B. welche Form die Stiftung haben soll, wie die angedachten Aufgaben der Stiftung ausgestaltet werden, wie sich die Finanzierung der Stiftung zusammensetzt und ob die Stiftung unabhängig tätig werden kann. Nicht zuletzt stellen sich Fragen der Kooperation und Zusammenarbeit mit den Datenschutzbehörden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für angezeigt, dass sie möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen werden. Auch sollte eine Bundesstiftung Datenschutz die bewährte föderale Struktur der Datenschutzaufsicht in Deutschland nicht beeinträchtigen.

Im Bereich der Bildung und Stärkung des Datenschutzbewusstseins stellen die Datenschutzbeauftragten bereits jetzt mit Broschüren, Merkblättern, eigenen

212 Zum Beschäftigtendatenschutz vgl. 2.1

213 Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Förderung des Datenschutzes durch Bundesstiftung, vgl. Dokumentenband 2010, S. 21

214 Allerdings gibt es ein Eckpunktepapier der FDP-Bundestagsabgeordneten Gisela Piltz zur Errichtung einer Stiftung Datenschutz, deren Aufgaben sich in vier Säulen gliedern.

Internetauftritten und mit dem „Virtuellen Datenschutzbüro“[215] Informationsmaterial für die Menschen sowie die nicht öffentlichen und öffentlichen Stellen zur Verfügung. Wenn die Stiftung diese Bemühungen unterstützt und die Bildungsangebote erweitert, ergänzt bzw. zusammenführt, kann dies nur von Vorteil sein. Auch die Idee, verschiedene Produkte und Dienstleistungen unter dem Aspekt des Datenschutzes im Wege vergleichender Tests gegenüberzustellen, ist sinnvoll. Die Datenschutzbehörden können den Testbereich nicht ausreichend abdecken. Die Erfahrungen aus anderen Testbereichen, z. B. mit der Stiftung Warentest, zeigen aber, dass solche Tests für die Wirtschaft starke Anreize schaffen, Produkte zu verbessern und sich von Wettbewerbern abzuheben. Datenschutz könnte dadurch zum Verkaufsargument werden. Im Zusammenhang mit der Vergabe von Gütesiegeln und Audits ist für eine Kooperation und Zusammenarbeit zwischen Stiftung und Datenschutzbehörden von zentraler Bedeutung, wie sich diese Tätigkeiten auf die Prüf- und Kontrolltätigkeit der Behörden auswirken können. Gütesiegel- und Audit-Verfahren sind Instrumente der Selbstregulierung, die nur funktionieren, wenn auch effektive Kontrollmechanismen bestehen. Eine Stärkung des Datenschutzes kann jedenfalls nicht dadurch erreicht werden, dass aufgrund eines Siegels oder Audits Folgekontrollen durch die staatliche Aufsicht beschränkt werden. Sollen von solchen Zertifizierungen allerdings Bindungswirkungen auch für die Kontrollbehörden ausgehen, ist es unerlässlich, dass die Datenschutzbeauftragten bei der Konzeption der Siegelkriterien und des -verfahrens sowie beim Zertifizierungsprozess eingebunden werden. Zudem sollte der Bundesgesetzgeber den seit 2001 bestehenden **Auftrag**[216] **zum Erlass eines Ausführungsgesetzes zum Datenschutzaudit** erfüllen.

Die im Koalitionsvertrag vorgesehenen Aufgaben können nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nur unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrgenommen werden. Die Konzeption der Stiftung Datenschutz als unabhängige Zertifizierungs-, Test- und Bildungsstelle berührt auch Fragen der Finanzierung. Im Bundeshaushalt 2011 sind 10 Millionen Euro für die Stiftung Datenschutz veranschlagt worden[217]. Darüber hinaus ist noch ungeklärt, ob und welche Gelder bereitgestellt werden, insbesondere ob die Wirtschaft die Stiftung mitfinanzieren soll. Letzteres könnte ihre Unabhängigkeit gefährden.

Es bleibt abzuwarten, ob das mit der Stiftung Datenschutz angestrebte Ziel – die Stärkung des Datenschutzes – erreicht werden kann. Vieles hängt von der konkreten Konzeption der Stiftung ab.

12.2 Informationspflicht bei Datenpannen

Seit September 2009 gilt die mit der Novellierung des BDSG eingeführte Informationspflicht bei unrechtmäßiger Kenntniserlangung durch Dritte[218]. Diese Pflicht betrifft nur nicht öffentliche Stellen, z. B. Unternehmen, Vereine, Verbände, und solche öffentlichen Unternehmen, die mit privaten Unternehmen im Wettbewerb stehen.[219] Sie müssen sowohl die Datenschutzbehörde als auch die Betroffenen benachrichtigen, wenn bestimmte Daten[220] Dritten entweder durch Übermittlung oder auf sonstige Weise unrechtmäßig zur Kenntnis gelangen. Dies gilt unter der Voraussetzung, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die Betroffenen sind grundsätzlich einzeln zu benachrichtigen. Soweit dies nur mit unverhältnismäßigem Aufwand zu realisieren ist, ersetzt die Information der Öffentlichkeit die Individualbenachrichtigung. Dabei muss die verantwortliche Stelle entweder über Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, gleich wirksame Maßnahme die Öffentlichkeit informieren. Ein Verstoß gegen die neue Informationspflicht ist bußgeldbewehrt. Erfolgt die Mitteilung gegenüber der Aufsichtsbehörde oder den Betroffenen vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, kann die Aufsichtsbehörde ein Bußgeldverfahren einleiten und ein Bußgeld in Höhe von bis zu 300.000 Euro verhängen.[221]

215 Zentrales Portal der Datenschutzbehörden: www.datenschutz.de
216 Vgl. § 9a BDSG
217 BT-Drs. 17/3523, S. 28, und BT-Drs. 17/3325, S. 61/62

218 § 42a BDSG
219 Zur Informationspflicht von öffentlichen Stellen Berlins vgl. § 18 a BlnDSG, GVBl. 2011, S. 51
220 Dazu gehören besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG, Daten, die durch ein Berufsgeheimnis geschützt sind, Daten, die sich auf strafbare oder bußgeldbewehrte Handlungen beziehen, und Daten zu Bank- und Kreditkartenkonten.
221 § 43 Abs. 2 Nr. 7, Abs. 3 BDSG

Entsprechende Informationspflichten für den Verlust von Bestands-, Nutzungs- oder Verbindungsdaten gelten nach dem Telekommunikationsgesetz (TKG)[222] und dem Telemediengesetz (TMG)[223]. Für Daten, die dem Sozialgeheimnis[224] unterliegen, gilt seit August eine spezielle Informationspflicht[225], die sich auf besondere Arten personenbezogener Daten[226] bezieht.

In der Praxis zeigt sich bei der Anwendung der Neuregelung eine gewisse Unsicherheit. Den Unternehmen bereitet es insbesondere Schwierigkeiten einzuschätzen, wann von einer Kenntniserlangung durch Dritte auszugehen ist und wann schwerwiegende Beeinträchtigungen für die Rechte oder Interessen der Betroffenen zu erwarten sind. Bei der Entscheidung über die Form der Benachrichtigung – individuell oder durch Information der Öffentlichkeit – sind bisher keine größeren Probleme aufgetreten. Fast scheint es, als würden die Unternehmen eine individuelle Benachrichtigung grundsätzlich vorziehen, da die Information der Öffentlichkeit auch mit einem Imageschaden verbunden sein kann. Um die Daten verarbeitenden Stellen zu unterstützen, informationspflichtige Vorfälle zu identifizieren und die daraus folgenden Handlungspflichten umzusetzen, haben wir ein Merkblatt in Form von „Häufig gestellten Fragen“ (FAQs) veröffentlicht.[227] In mehreren Fällen haben wir uns zum konkreten Umfang der neuen Informationspflicht geäußert.

12.2.1 Datenklau beim Kreditkartendienstleister

Eine Bank beauftragte einen Dienstleister mit der Prägung und Versendung von Kreditkarten und PIN-Informationen an die Kundinnen und Kunden. Dieser Dienstleister schaltete einen Unterauftragnehmer ein, der wiederum einen weiteren Subauftragnehmer mit der Erledigung der Aufgaben betraute. Die Bank unterrichtete uns davon, dass ein Mitarbeiter des Subunternehmers verhaftet wurde und bei der Durchsuchung von Wohnung und Arbeitsplatz Kreditkartendaten sichergestellt worden seien. Wie uns die Bank mitteilte, hatte sich herausgestellt, dass der Mitarbeiter Doubletten von Kreditkarten gedruckt und PIN-Briefe gestohlen hatte, um mit den Karten Geld an Geldautomaten abheben zu können. Auch sog. Prägespurdaten, d. h. Daten, die auf der Karte gespeichert werden, wurden auf dem Rechner des Mitarbeiters gefunden. Die Daten hatte er offensichtlich mitgenommen, um Doubletten zu Hause nachzuprägen. Die Bank tauschte sämtliche Kreditkarten aus, zu denen Doubletten beim Beschuldigten sichergestellt wurden. Zuvor hatte sie die Kundinnen und Kunden schriftlich auf auffällige Umsätze bei der Prüfung der Transaktionsdaten hingewiesen; sie hatten daraufhin mit der Bank Kontakt aufgenommen. Kundinnen und Kunden, zu denen allein Prägespurdaten sichergestellt wurden, benachrichtigte die Bank nicht.

Die entwendeten Daten sind personenbezogene Daten zu Kreditkarten- und Bankkonten, die einem Dritten unrechtmäßig zur Kenntnis gelangt waren. Der Mitarbeiter nutzte die Daten zu anderen als im Rahmen seiner Tätigkeit vorgesehenen Zwecken, sodass er die Daten nicht als Mitarbeiter, sondern als „Dritter“ verwendete. Die Bank hatte zu prüfen, ob sie nach § 42a BDSG verpflichtet war, die Betroffenen zu benachrichtigen. Dafür musste sie prognostizieren, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen durch das Handeln des Beschuldigten drohten. Die Bank stellte sich auf den Standpunkt, dass dies nicht der Fall sei: Für die Zukunft schloss sie eine missbräuchliche Verwendung der Daten aus, da die Karten, zu denen Doubletten vorhanden waren, ausgetauscht worden waren. Zudem kam die Bank zu dem Ergebnis, dass keine weiteren als die bekannten Schadensfälle zu erwarten seien. In Bezug auf die Prägespurdaten wies sie darauf hin, dass es dem Beschuldigten nicht gelungen war, diese auf Doubletten zu drucken und die Karten dann zu verwenden. Darüber hinaus schloss die Bank es als unwahrscheinlich aus, dass der Beschuldigte die Prägespurdaten für Bestellungen im Internet verwendet oder an (Mit-)Täter weitergegeben hatte. Dies konnte sie insbesondere anhand der Ergebnisse des strafrechtlichen Ermittlungsverfahrens nachvollziehbar darlegen. Wir hatten keine Anhaltspunkte, an dieser Einschätzung zu zweifeln.

222 § 93 Abs. 3 TKG
223 § 15a TMG
224 § 35 Sozialgesetzbuch (SGB) I, § 67 SGB X
225 § 83a SGB X
226 § 67 Abs. 12 SGB X
227 http://www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg

Für die betroffenen Stellen ist es hilfreich, Szenarien zu entwerfen, wie die Daten genutzt werden könnten. Solche Szenarien sind daraufhin zu analysieren, welche Beeinträchtigungen der Betroffenen materieller wie immaterieller Art (z. B. Vermögensschäden, soziale Nachteile) möglich sind und wie wahrscheinlich deren Eintritt ist. Je größer die mögliche Beeinträchtigung ist, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen. Die betroffenen Stellen sollten den Entscheidungsprozess dokumentieren und das prognostizierte Ergebnis nachvollziehbar begründen können.

12.2.2 Gestohlene Laptops einer Kinderbetreuungseinrichtung

Eine Kinderbetreuungseinrichtung meldete uns den Diebstahl von drei Notebooks, die sowohl zur Verwaltung der Kundendaten als auch für Zwecke der Dokumentation der Kinderbetreuung eingesetzt wurden. Auf den Laptops waren u. a. Kontodaten der Kundinnen und Kunden sowie Beobachtungs- und Eingewöhnungsprotokolle zu den betreuten Kindern und Dokumente zu Elterngesprächen gespeichert. Eines der Notebooks wurde aus einem Fahrzeug gestohlen. Die anderen beiden Laptops befanden sich zum Zeitpunkt des Diebstahls im verschlossenen Gebäude der Einrichtung. Sie hatte die betroffenen Eltern bereits unterrichtet, bevor sie uns über die Vorfälle informierte.

Auf die Frage, ob die Kinderbetreuungseinrichtung überhaupt verpflichtet war, die Betroffenen zu unterrichten, kam es nicht an, denn sie hatte die Informationspflicht gegenüber den Betroffenen bereits erfüllt, bevor sie uns benachrichtigte. Gleichwohl meinte sie, dass eine Informationspflicht nicht bestanden hätte: Ihr sei nicht bekannt geworden, ob die Diebe der Laptops die gespeicherten Daten tatsächlich zur Kenntnis genommen haben.

Die Kenntniserlangung durch einen Dritten muss von der betroffenen Stelle nicht positiv festgestellt werden. Es reicht aus, wenn es entweder offensichtlich ist, dass Dritte Kenntnis erlangt haben, oder wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann. Bei gestohlenen Laptops ist dies jedenfalls dann anzunehmen, wenn die Festplatten bzw. die Daten (wie im vorliegenden Fall) nicht verschlüsselt

waren. Eine Zugangssperre (etwa in Form des Windows-Login) reicht nicht aus. Diese kann technisch leicht umgangen werden.

Beim Einsatz von mobilen Geräten ist generell zu empfehlen, Verschlüsselungsmechanismen einzusetzen, insbesondere die Festplatten zu verschlüsseln. Darüber hinaus sollten Laptops mit personenbezogenen Daten über das Fahrtende hinaus nicht in Fahrzeugen aufbewahrt werden.

12.2.3 Personalakten im Posteingang

Ein Unternehmen ließ Personalakten von einem externen Dienstleister im Wege einer Datenverarbeitung im Auftrag[228] digitalisieren. Nach dem Einscannen lieferte dieser die digitalisierten Akten in verplombten Behältnissen an das Unternehmen zurück. Entgegen der Absprache wurden die Kisten nicht direkt beim zuständigen Mitarbeiter der Personalabteilung abgegeben, sondern gelangten in den normalen Posteingang, wo sie geöffnet wurden. Das Unternehmen teilte uns mit, dass die Mitarbeiter nur die Aktenvorblätter und Registerblätter einsahen. Den Vorblättern waren keine personenbezogenen Daten im Klartext, sondern nur in Form eines Barcodes zu entnehmen. Dieser war für die Mitarbeiter des Posteingangs nicht auflösbar. Anhand der Vorblätter konnten sie bereits feststellen, dass es sich um Personalakten handelte, da allseits bekannt war, dass ausschließlich Personalakten gescannt wurden. Die Aktenstapel wurden von den Mitarbeitern daraufhin nicht geöffnet, und es wurde keine Einsicht in einzelne Akten genommen.

Das Unternehmen war nicht verpflichtet, die Betroffenen zu benachrichtigen. Es bestanden keine tatsächlichen Anhaltspunkte dafür, dass die Mitarbeiter des Posteingangs Daten im Sinne von § 42a BDSG zur Kenntnis genommen hatten. Grundsätzlich müssen Unternehmen auch bei Personaldaten prüfen, ob die Betroffenen zu benachrichtigen sind. Personalakten können besondere Arten personenbezogener Daten enthalten (wie Informationen zur Religionszugehörigkeit oder Krankschreibungen). Darüber hinaus können Daten zur Bankver-

228 § 11 BDSG

bindung in Personalakten gespeichert sein. Auch könnten Akten einem Berufsgeheimnis unterliegen. Für die Pflicht zur Benachrichtigung kommt es nicht darauf an, dass die Daten außerhalb des Unternehmens stehenden Personen unberechtigt zur Kenntnis gelangt sind.

Die Unternehmen können auch dann verpflichtet sein, die Betroffenen zu benachrichtigen, wenn Daten intern an nicht berechtigte Beschäftigte weitergegeben werden.

12.2.4 Kreditverträge im Auto

Eine Tasche mit Kreditverträgen zweier Kunden wurde aus dem Pkw eines Bankangestellten gestohlen. Die Bank benachrichtigte die Kunden über den Verlust der Verträge. In einer Richtlinie hatte die Bank organisatorisch festgelegt, dass vertrauliche Unterlagen außerhalb des Bankgebäudes nicht aus der Hand gegeben oder ohne persönliche Aufsicht gelagert werden dürfen. Gleichwohl hatte der Mitarbeiter dagegen verstoßen.

Die Bank erfüllte ihre Informationspflichten gegenüber der Aufsichtsbehörde und den Betroffenen ordnungsgemäß. Wir haben die Bank darauf hingewiesen, dass den Betroffenen angeboten werden sollte, die Bankverbindung zu wechseln, wenn diese aus den Unterlagen hervorging. Sollten Maßnahmen existieren, die mögliche nachteilige Folgen des Datenverlustes mindern, sind diese dem Betroffenen bei der Benachrichtigung mitzuteilen.

Organisatorische Festlegungen entbinden betroffene Stellen bei einem Datenverlust nicht von der Informationspflicht.

12.3 WLAN-Einsatz in der Berliner Verwaltung

Aufgrund kostengünstiger Komponenten, des geringen Installationsaufwands und der Kompatibilität mit vorhandenen Netzstrukturen hat der Betrieb lokaler Funknetze (Wireless Local Area Networks (WLANs)) nach dem IEEE 802.11-Standard zugenommen. Sie erhöhen die Mobilität, sind flexibel und im Vergleich zu drahtgebundenen Vernetzungen schneller und kostengünstiger aufzubauen, da keine physisch vorhandenen Leitungsanschlüsse benötigt werden. Da jedoch als Trägermedium für die zu transportierenden Daten Funkwellen genutzt werden, sind Angriffe auf die Daten auch ohne räumlichen Zugriff möglich. Die bisher oft anzutreffende mangelhafte Sicherheit – z. B. der Einsatz des unsicheren WEP-Verfahrens zur Datenverschlüsselung – gefährdet die Datensicherheit ganzer Netze, obwohl es eine Vielzahl von Maßnahmen für den sicheren Einsatz von WLANs gibt. Wir haben schon früher zu Datenschutz- und Datensicherheitsproblemen in lokalen Funknetzen berichtet[229]. In diesem Zusammenhang hatten wir z. B. auf die Notwendigkeit der Verschlüsselung mit WPA2-AES oder der Ersteinrichtung per Kabel sowie der Vergabe eines individuellen Passwortes für den Router hingewiesen.

Um einen aktuellen Überblick über den Stand des Einsatzes von WLANs in den Bezirksämtern und Senatsverwaltungen zu erhalten, haben wir um Beantwortung eines Fragenkatalogs gebeten. Er enthält auch Fragen zum Vorhandensein einer Sicherheitsrichtlinie, zur Erstellung eines Sicherheitskonzepts, zum Einsatz von Verschlüsselungsverfahren und zur Änderung von Standardkennwörtern. Die nach Auswertung der Fragebögen durchgeführten (und noch andauernden) Kontrollen erstrecken sich auf das Vorhandensein von Funknetzen in den öffentlichen Stellen und deren Umgebung. Als Zwischenstand kann zu den bisher kontrollierten Standorten ein positives Fazit gezogen werden, da man offensichtlich aus den Fehlern der Vergangenheit gelernt hat und z. B. ausschließlich der sichere WPA2-Verschlüsselungsstandard vorgefunden wurde.

Die Kontrollen dienen ausschließlich dem Zweck, dass evtl. installierte WLANs im öffentlichen Bereich aufgefunden werden. Hierbei soll festgestellt werden, ob und wenn ja welche Sicherheitsmaßnahmen beim Einsatz der Informationstechnik ergriffen wurden. Es werden keine eigenen Penetrationsversuche

229 Zuletzt JB 2005, 4.9.4

in WLANs erfolgen, auch dann nicht, wenn eine unzureichende Absicherung vorliegt (z. B. bei einem nur mit WEP geschützten WLAN). Außerdem werden auch keine standortbezogenen Angaben (z. B. mit GPS) festgehalten.

Für die Kontrollen werden ein Notebook, Netbook, Smartphone und PDA mit den frei verfügbaren oder kommerziellen Softwaretools Netstumbler, inSSIDer, WiFiFoFum2 eingesetzt. Netstumbler ist ein WLAN-Monitor-Programm (Scanner) für Windows. Es prüft die WLAN-Kanäle, ob darauf Netzwerke (Wireless Access Points (AP) nach dem Standard 802.11a, b und g) verfügbar sind. Es liefert detaillierte Informationen (wie Netzwerkname, MAC-Adresse, ob Verschlüsselung oder nicht). Außerdem sucht es aktiv die Netzwerke durch regelmäßiges Senden von Probe-Anfragen. Ist der AP so konfiguriert, dass er auf diese Anfrage reagiert, kann Netstumbler ihn erkennen. Andernfalls taucht der AP nicht in der Liste auf; man spricht dann von einem sog. closed AP. Auch inSSIDer und WiFiFoFum haben einen vergleichbaren Funktionsumfang, zeigen jedoch nicht nur an, dass eine Verschlüsselung erfolgt, sondern erkennen auch das verwendete Verschlüsselungsverfahren.

Funknetze kennen keine räumlichen Grenzen. Die Orientierungshilfe „Datenschutz in drahtlosen Netzen“[230] steht Interessierten im Internet zur Verfügung.[231]

12.4 Ein Beauftragter für behördlichen Datenschutz und Korruptionsbekämpfung?

Nachdem wir festgestellt hatten, dass sowohl das Amt des behördlichen Datenschutzbeauftragten als auch das Amt des Antikorruptionsbeauftragten beim Bezirksamt Pankow von derselben Person ausgeübt wurden, wiesen wir das Bezirksamt auf die Unvereinbarkeit beider Ämter hin. Das Bezirksamt erklärte, dass der behördliche Datenschutzbeauftragte am besten beurteilen könne, welche datenschutzrechtlichen Bestimmungen für die Arbeit des Antikorruptionsbeauftragten gelten. Die Ämterkombination befähige zu einem verantwortungsvollen Umgang mit den jeweils zugewiesenen Aufgaben. Auch sehe sich die betreffende Person selbst keinem Interessenkonflikt zwischen seinen Aufgaben als behördlicher Datenschutz- und Antikorruptionsbeauftragter ausgesetzt.

230 Sie wurde erstellt von den Arbeitskreisen „Technische und organisatorische Datenschutzfragen“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

231 www.lfd.m-v.de/dschutz/informat/wlan/oh_wlan.pdf

Nach dem Gesetz darf zum behördlichen Datenschutzbeauftragten nur bestellt werden, wer durch die Bestellung keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird[232]. Hier besteht ein solcher Interessenkonflikt: Der behördliche Datenschutzbeauftragte hat einerseits die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen, andererseits hat er als Antikorruptionsbeauftragter die Aufgabe, u.a. durch Erhebung und Verarbeitung von personenbezogenen Daten in umfangreichem Maß Korruption zu bekämpfen bzw. vorzubeugen. Durch die ihm übertragene Doppelfunktion liegen Entscheidungs- und Kontrollfunktion in einer Hand. Der Datenschutzbeauftragte müsste seine eigene Arbeit als Antikorruptionsbeauftragter kontrollieren. Die Unabhängigkeit, die ein behördlicher Datenschutzbeauftragter zur ordnungsgemäßen Erfüllung seiner Aufgaben benötigt, ist so nicht gewährleistet. Dass die betreffende Person die Ansicht vertritt, ein Interessenkonflikt bestehe nicht, ist nicht ausschlaggebend für die Bewertung der Rechtmäßigkeit seiner Bestellung zum behördlichen Datenschutzbeauftragten.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die Praxis des Bezirksamts beanstandet und empfohlen, die betreffende Person von einer der beiden Funktionen zu entbinden, um den bestehenden Interessenkonflikt zu beenden. Das Bezirksamt ist dieser Empfehlung nicht gefolgt.

Die Funktionen des behördlichen Datenschutzbeauftragten und des Antikorruptionsbeauftragten sind nicht miteinander vereinbar. Sie müssen von unterschiedlichen Personen wahrgenommen werden.

232 § 19 a Abs. 2 Satz 1 BlnDSG

13. Telekommunikation und Medien

13.1 Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat im März über die zahlreichen Verfassungsbeschwerden gegen die Einführung der sog. „Vorratsdatenspeicherung“[233] entschieden. Mit ihr wurden Anbieter von Telekommunikationsdienstleistungen verpflichtet, Verkehrsdaten für die Dauer von sechs Monaten anlassunabhängig für Zwecke der Strafverfolgung zu speichern und den Strafverfolgungsbehörden und Nachrichtendiensten im Einzelfall für die Erfüllung ihrer Aufgaben zu übermitteln.

In einer einstweiligen Anordnung[234] hatte das Bundesverfassungsgericht bereits zwei Jahre zuvor bestimmt, dass die zur Vorratsdatenspeicherung verpflichteten Anbieter von Telekommunikationsdienstleistungen bis zum Abschluss des Hauptverfahrens Vorratsdaten an die ersuchende Behörde nur dann übermitteln dürfen, wenn gemäß der Anordnung des Abrufs der Gegenstand des Ermittlungsverfahrens eine Katalogtat nach § 100 a Abs. 2 Strafprozessordnung (StPO) ist und die Voraussetzungen des § 100 a Abs. 1 StPO vorliegen. Dagegen sei in den Fällen des § 100 g Abs. 1 StPO von einer Übermittlung der Vorratsdaten an die Ermittlungsbehörden vorläufig abzusehen.

In einer weiteren einstweiligen Anordnung hatte das Bundesverfassungsgericht die Nutzung der Vorratsdaten im Bereich der Gefahrenabwehr auf die Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr beschränkt.[235]

Im Verlauf des Verfahrens hatte das Bundesverfassungsgericht die Landesbeauftragten für den Datenschutz um eine Stellungnahme zu den Verfassungsbeschwerden gebeten, die wir unter den Landesbeauftragten abgestimmt und in deren Namen abgegeben haben. Darin haben wir unsere Auffassung dargelegt, dass die §§ 113 a, 113 b TKG das Fernmeldegeheimnis aus Art. 10 GG in seinem Wesensgehalt verletzen. Die angegriffenen Regelungen verstießen darüber hinaus auch gegen das Verbot der Vorratssammlung zu unbestimmten oder noch nicht bestimmbaren Zwecken und ermöglichten eine unverhältnismäßige Einschränkung des Fernmeldegeheimnisses.

Dieser Auffassung hat sich das Bundesverfassungsgericht nur teilweise angeschlossen: Das Gericht hat zwar die in den Verfassungsbeschwerden angegriffenen §§ 113 a, 113 b TKG und § 100 g Abs. 1 Satz 1 StPO, soweit danach Verkehrsdaten erhoben werden dürfen, für nichtig erklärt und angeordnet, dass die aufgrund der einstweiligen Anordnungen von den Diensteanbietern noch nicht an die ersuchenden Behörden übermittelten Telekommunikationsverkehrsdaten unverzüglich gelöscht werden müssen.[236]

Das Gericht führt jedoch aus, dass eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter mit dem Fernmeldegeheimnis in Art. 10 GG *„nicht schlechthin unvereinbar“* ist; insbesondere verletze sie nicht dessen Wesensgehalt. Allerdings sieht das Bundesverfassungsgericht in dieser Vorratsdatenspeicherung einen *„besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. […] Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist.“*[237] Weiter heißt es in dem Urteil plastisch: *„Hierdurch ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte beeinträchtigen kann.“*[238] Deshalb ist die konkrete Umsetzung der Vorschriften der Richtlinie 2006/24/EG durch die Bundesregierung in nationales Recht[239] nach Auffassung des Bundesverfassungsgerichts mit Art. 10 Abs. 1 GG nicht vereinbar. Das betrifft insbesondere die Vorschriften zum

233 Vgl. JB 2007, 12.1.1
234 Beschluss vom 11. März 2008 – 1 BvR 56/08
235 Beschluss vom 28. Oktober 2008 – 1 BvR 256/08
236 Urteil vom 2. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, S. 833 ff.
237 Ebenda, S. 838, Rn. 210
238 Ebenda, Rn. 212
239 Vgl. Gesetz zur Neuregelung der Telekommunikationsüberwachungen und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007, BGBl. I, S. 3198

Abruf und zur unmittelbaren Nutzung der gespeicherten Daten: Diese hält das Bundesverfassungsgericht nur für verhältnismäßig, wenn sie *„überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen“*. Voraussetzung hierfür ist im Bereich der Strafverfolgung ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat.[240] Eine Nutzung für Zwecke der Gefahrenabwehr und der Nachrichtendienste darf nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr ermöglicht werden.[241] Auch die Regelungen zur Datensicherheit hält das Bundesverfassungsgericht für unzureichend und fordert wegen des Umfangs und der potenziellen Aussagekraft der Daten einen besonders hohen Standard.[242] Auch müssten die Vorschriften zur Erteilung von Auskünften über Inhaber von IP-Adressen so gefasst werden, dass sie zukünftig für die Verfolgung von Ordnungswidrigkeiten nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt ist.

Die Bundesregierung hat bisher keinen neuen Entwurf zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung vorgelegt. Auf europäischer Ebene läuft gegenwärtig eine Evaluation dieser Richtlinie. Die Veröffentlichung der Ergebnisse ist bereits mehrfach verschoben worden und jetzt für das Frühjahr 2011 angekündigt. In mehreren anderen EU-Mitgliedstaaten ist die Richtlinie bisher nicht umgesetzt oder ihre Umsetzung von Gerichten gestoppt worden. Der Europäische Gerichtshof muss sich auf Vorlage des irischen High Court mit der Frage befassen, ob die Richtlinie zur Vorratsdatenspeicherung mit den in der EU geltenden Grundrechten vereinbar ist. Die Art. 29-Datenschutzgruppe hat die Umsetzung der Richtlinie in den Mitgliedstaaten untersucht und sich für eine Verkürzung der Höchstfrist für die Vorratsdatenspeicherung und die Einführung einer einheitlichen, kürzeren Frist ausgesprochen. [243]

240 BVerfG, Entscheidung vom 2. März 2010 – 1 BvR 296/08, Nr. 228
241 Ebenda, Nr. 231
242 Ebenda, Nr. 221 ff.
243 Vgl. Bericht 01/2010 vom 13. Juli 2010 (WP 172) über die zweite gemeinsame Durchsetzungsmaßnahme: Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten aufgrund der Art. 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (über die Vorratsspeicherung von Daten und zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation) bestehenden Pflichten durch die Telekommunikations-Diensteanbieter und die Internet-Diensteanbieter auf nationaler Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Bundesregierung aufgefordert, sich für eine Aufhebung der Europäischen Richtlinie zur Vorratsdatenspeicherung einzusetzen.[244] Auch hat sie darauf hingewiesen, dass der Gesetzgeber nach dem Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung bei der Einführung neuer Speicherpflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen ist.

Die Bundesregierung sollte sich auf europäischer Ebene für eine Aufhebung der Richtlinie zur Vorratsdatenspeicherung einsetzen. Sollte dies nicht zum Erfolg führen, muss die Richtlinie jedenfalls grundrechtsschonend in nationales Recht umgesetzt werden.

13.2 Soziale Netzwerke

Trotz der vom Betreiber nach dem letzten Vorfall dieser Art[245] getroffenen Schutzmaßnahmen ist es wieder zu einem massenweisen Auslesen von Profildaten aus dem sozialen Netzwerk SchülerVZ gekommen: Einem Studenten war es gelungen, 1,6 Millionen Profildatensätze aus dem Netzwerk automatisiert auszulesen.

Wir haben uns die vom Betreiber zusätzlich getroffenen Schutzmaßnahmen schildern lassen. Auch hier waren wiederum „nur“ Daten ausgelesen worden, die von den Betroffenen so konfiguriert waren, dass jedes Mitglied der Plattform sie einsehen durfte. Die nach dem Vorfall durch den Anbieter ergänzend getroffenen Sicherungsmaßnahmen halten wir im Ergebnis für ausreichend. Es kann jedoch nicht ausgeschlossen werden, dass derartige Angriffe auch zukünftig mit geänderten Vorgehensweisen oder unter Nutzung bisher noch nicht bekannter Sicherheitslücken erfolgreich wiederholt werden. Wir empfehlen daher schon seit Langem, die Veröffentlichung personenbezogener

244 Entschließung vom 17./18. März 2010: Keine Vorratsdatenspeicherung!, vgl. Dokumentenband 2010, S. 13
245 Vgl. JB 2009, 13.1

Daten auf ein Minimum zu beschränken und mithilfe der Privatsphäre-Einstellungen den Zugriff auf solche Daten auf einen möglichst kleinen Personenkreis zu begrenzen. Darüber hinaus sollten die Nutzenden in sozialen Netzwerken nicht unter dem Klarnamen, sondern unter einem Pseudonym (Spitznamen) auftreten.[246] Diese Botschaft scheint erfreulicherweise zunehmend auch bei jugendlichen Nutzenden anzukommen: Laut einer im November publizierten Umfrage stellen Jugendliche inzwischen weniger personenbezogene Daten im Netz zur Verfügung und machen zunehmend auch von Einstellmöglichkeiten zur Begrenzung von deren Verfügbarkeit Gebrauch.[247]

Viele soziale Netzwerke bieten Nutzenden eine aus Datenschutzsicht umstrittene Möglichkeit, eigene Bekannte innerhalb des Netzwerks aufzufinden **(„Friendfinder“)**: Dazu erlaubt die oder der Nutzende dem Netzwerkbetreiber kurzzeitig den Zugriff auf das E-Mail-Adressbuch eines Web-E-Mail-Dienstes oder eines Smartphones, damit der Netzwerkbetreiber die vorgefundenen E-Mail-Adressen mit denen der Mitglieder des Netzwerks abgleichen kann. Mit den so aufgefundenen Profilen von Bekannten kann man sich vernetzen oder anderen, die noch nicht Mitglied des Netzwerks sind, eine Einladung schicken.

In Verruf gekommen ist diese Funktion, weil einige Netzwerke die Daten auch von Nicht-Mitgliedern und deren Beziehungen untereinander, die sich aus der Eintragung im selben E-Mail-Adressbuch ergeben, dauerhaft abspeichern und für eigene Marketingzwecke verwenden, ohne dass die Inhaber der E-Mail-Adressen eine entsprechende Einwilligung erteilt haben. Das führt dazu, dass auch solche Personen unaufgefordert Werbemails von Netzwerken bekommen, in denen sie nicht Mitglied sind. Diese Netzwerke entwickeln so eine zusätzliche Sogwirkung. Eine derartige Praxis verstößt gegen deutsches und europäisches Datenschutzrecht.

246 Vgl. die von jugendnetz-berlin.de und uns herausgegebene Broschüre zu sozialen Netzwerken und Datenschutz „Ich suche Dich. Wer bist du?“; http://www.datenschutz-berlin.de/attachments/626/Broschuere_Soziale_Netzwerke_Ich_suche_dich.pdf?1255923610

247 Medienpädagogischer Forschungsverbund Südwest (Hrsg.): JIM-Studie 2010, Jugend, Information, (Multi-) Media, Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland (S. 44 f.), abrufbar unter http://www.mpfs.de

Bei den VZ-Netzwerken werden nach Aussagen des Unternehmens E-Mail-Adressen ausschließlich für den von den Nutzenden gewünschten Abgleich oder zum Senden von Einladungen genutzt und nicht dauerhaft gespeichert. Allerdings bestand in der Vergangenheit das Problem, dass Pseudonyme von bereits registrierten Nutzenden unter bestimmten Umständen aufgedeckt werden konnten, wenn den Nutzenden aufgrund der E-Mail-Adresse Profildaten der in einem Netzwerk gefundenen Bekannten angezeigt wurden. Die VZ-Netzwerke haben dieses Problem nach unserem Hinweis unverzüglich so gelöst, dass die oder der Einladende erst bei einer Freundschaftsbestätigung von Profildaten der oder des Bekannten erfährt. Wir empfehlen ohnehin, für die Nutzung sozialer Netzwerke eine gesonderte E-Mail-Adresse zu verwenden, die nur für diesen Zweck und nicht in anderen Zusammenhängen eingesetzt wird.

Weiterhin steigender Beliebtheit erfreuen sich auch in sozialen Netzwerken von Dritten angebotene **Anwendungsprogramme („Apps“)**[248]. Dabei handelt es sich vielfach um Spiele, es existiert aber auch eine Vielzahl anderer Anwendungen. Viele dieser Programme benötigen für den Betrieb den Zugriff auf persönliche Daten der Nutzenden (bei Spielen ist dies z. B. dann der Fall, wenn man mit seinen oder gegen seine Freunde spielen möchte). Bei der Nutzung solcher Drittanwendungen ist insbesondere zu beachten, dass diese Angebote überwiegend von Anbietern zur Verfügung gestellt werden, die nicht identisch mit dem Betreiber des sozialen Netzwerks sind. Sie können darüber hinaus ihren Sitz in einer Rechtsordnung haben, die von der des Anbieters abweicht. Insofern ist nicht sichergestellt, dass auch für die Anbieter der Anwendungen dasselbe Datenschutzrecht gilt wie für den Betreiber des sozialen Netzwerks. Vielfach sind Anbieter von Drittanwendungen auch in Ländern außerhalb des Europäischen Wirtschaftsraums angesiedelt, in denen kein ausreichendes Datenschutzniveau gegeben ist. Teilweise fehlt es in diesen Ländern auch an einer wirksamen Datenschutzaufsicht. Wir raten daher allen, die solche Drittanwendungen nutzen wollen, sich vor der Nutzung über die für die Anwendung geltenden Datenschutzbedingungen einschließlich des Sitzlandes des Anbieters zu informieren.

Auch gegenüber diesen Drittanbietern sollten die Nutzenden so weit wie möglich unter Pseudonym auftreten. Die VZ-Netzwerke unterstützen dies durch

248 Vgl. 2.5 (Apps bei Smartphones)

das Angebot „Visitenkarten“: Anwendungen von Drittanbietern haben keinen Direktzugriff auf die Profildaten der Nutzenden, sondern nur auf Daten, die die oder der Nutzende der jeweiligen Anwendung auf der Visitenkarte ausdrücklich zur Verfügung stellt. Dies ermöglicht insbesondere auch die Verwendung verschiedener Pseudonyme bei verschiedenen Drittanbietern.

Der Düsseldorfer Kreis hat auf die Notwendigkeit hingewiesen, insbesondere Minderjährige in sozialen Netzen wirksamer zu schützen.[249] Zu den empfohlenen Maßnahmen zählen datenschutzfreundliche Standardeinstellungen, die bei Minderjährigen besonders restriktiv gefasst werden sollten, die Einhaltung und wirksame Überprüfung von gesetzlich bzw. durch die Betreiber selbst vorgegebenen Grenzen für das Mindestalter der Nutzenden, eine freiwillige Alterskennzeichnung und die Aufklärung der Nutzenden über bestehende, datenschutzfreundliche Nutzungsmöglichkeiten.

Wer soziale Netzwerke nutzt, sollte Pseudonyme statt Klarnamen verwenden, die Veröffentlichung personenbezogener Daten auf ein Minimum beschränken und mithilfe der Privatsphäre-Einstellungen den Zugriff auf solche Daten möglichst eng begrenzen. Bei der Nutzung von Drittanwendungen sollte man sich unbedingt vorher über die für die Anwendung geltenden Datenschutzbedingungen einschließlich des Sitzlandes des Anbieters informieren.

13.3 Aus der Arbeit der „Berlin Group“

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

- Die „‘Granada Charta‘ des Datenschutzes in einer digitalen Welt“ formuliert Prinzipien, die Nutzenden, Anbietern und öffentlichen Stellen helfen sollen, einen freien Informationsfluss zu ermöglichen und gleichzeitig die Würde, die Privatsphäre und den Datenschutz von Individuen zu bewahren.[250]

249 Beschluss vom 24./25. November 2010, vgl. Dokumentenband 2010, S. 24
250 Dokumentenband 2010, S. 138

- Das Arbeitspapier „Mobile Verarbeitung personenbezogener Daten und Datensicherheit“ enthält Empfehlungen, um den besonderen Sicherheitsrisiken der Verarbeitung personenbezogener Daten auf mobilen Endgeräten zu begegnen.[251]
- Das Arbeitspapier zur Nutzung von „Deep Packet Inspection“ zu Marketing-Zwecken fordert Internet-Zugangsdiensteanbieter dazu auf, die Nutzung der Deep Packet Inspection-Technologie für zielgerichtete bzw. verhaltensbasierte Werbung zu unterlassen.[252]

Darüber hinaus ist das „Arbeitspapier zu Risiken für die Privatsphäre im Zusammenhang mit der Wiederverwendung von Email-Accounts und ähnlichen Diensten der Informationsgesellschaft“[253] überarbeitet und aktualisiert worden.[254]

13.4 Kein Systemwechsel bei der Rundfunkfinanzierung

Ab 2013 soll der öffentlich-rechtliche Rundfunk nicht mehr durch eine geräteabhängige Gebühr, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag finanziert werden. So sieht es die von den Ministerpräsidenten im Dezember beschlossene Fassung des 15. Rundfunkänderungsstaatsvertrags vor, der derzeit in den Länderparlamenten zur Abstimmung steht.

Die Idee, die Rundfunkgebührenpflicht nicht mehr an einzelne Personen, sondern an den jeweiligen Haushalt zu knüpfen, ist nicht neu. Bereits 2003 wurde über eine solche Neuordnung der Rundfunkfinanzierung diskutiert, jedoch nicht zuletzt aufgrund der Vorbehalte der Datenschutzbeauftragten des Bundes und der Länder davon Abstand genommen.[255]

251 Dokumentenband 2010, S. 149
252 Dokumentenband 2010, S. 147
253 Dokumentenband 2009, S. 153 ff.
254 Dokumentenband 2010, S. 142
255 JB 2003, 5.2; Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003: Neuordnung der Rundfunkfinanzierung, vgl. Dokumentenband 2003, S. 37 f.

Auch die aktuellen Planungen zur Neugestaltung der Rundfunkfinanzierung lassen diese Vorbehalte weitgehend unberücksichtigt.[256] Die langjährig kritisierte Praxis der umfangreichen Datenerhebung und -verarbeitung durch die GEZ und die Rundfunkgebührenbeauftragten soll noch erweitert und damit einhergehend der Umfang der Datensammlung vergrößert werden. So sieht der Staatsvertrag in Ergänzung zu den bisherigen Regelungen die Möglichkeit einer Datenerhebung bei einer unbegrenzten Anzahl von öffentlichen Stellen[257] ohne Kenntnis der Betroffenen vor. Lediglich vorübergehend soll auf die Nutzung von Datenbeständen des Adresshandels verzichtet werden, soweit sie „private Personen" betreffen.

Eine Loslösung vom Rundfunkbeitragseinzug durch die GEZ könnte diese Mängel ausräumen. Denkbar wäre etwa die Erhebung des Beitrags durch die Finanzämter. Dies hätte zur Folge, dass eine der größten zentralen Datenbanken Deutschlands abgeschafft und ein damit zwangsläufig erhöhtes Missbrauchspotenzial beseitigt würde.

Die geplante Neuordnung der Rundfunkfinanzierung stellt angesichts der Beibehaltung der Organisation des Beitragseinzugs durch die GEZ sowie der Ausweitung der Datenerhebungs- und -verarbeitungsbefugnisse keinen tatsächlichen Systemwechsel dar, sondern eine Verschlechterung gegenüber dem Ist-Zustand. Die Chance für einen datenschutzgerechten Neuanfang wurde damit vertan.

256 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010: Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!, vgl. Dokumentenband 2010, S. 17

257 Wie Finanzämtern, Agenturen für Arbeit, Polizei- und Straßenverkehrsbehörden

14. Informationsfreiheit

14.1 Informationsfreiheit in Berlin und Deutschland

Im ersten Halbjahr tagte die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) turnusgemäß unter unserem Vorsitz. In einer Entschließung[258] wies sie darauf hin, dass das Recht auf Informationszugang auch gegenüber den **öffentlich-rechtlichen Rundfunkanstalten** als Trägern mittelbarer Staatsverwaltung gilt, sofern nicht deren grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit berührt ist. Soweit nicht schon vorhanden, seien ausdrückliche Rechtsvorschriften zu schaffen, nach denen die jeweiligen Informationsfreiheitsgesetze auch auf die öffentlich-rechtlichen Rundfunkanstalten außerhalb der grundrechtlich garantierten Rundfunkfreiheit anzuwenden sind.[259]

Würde diese Forderung in Berlin umgesetzt, wäre ein jahrelanger Streit zwischen uns und dem **Rundfunk Berlin-Brandenburg** beigelegt.[260] Allerdings sehen weder der RBB noch die für das IFG federführend zuständige Senatsverwaltung für Inneres und Sport einen gesetzgeberischen Handlungsbedarf. Sie bezweifelt sogar, dass es „Ansatzpunkte" für eine Kontrolle des Verwaltungshandelns beim RBB geben kann. Dieser vertritt nun die Auffassung, dass nur für hoheitliche Tätigkeiten (wie die Zuteilung von Sendezeiten an politische Parteien und den Rundfunkgebühreneinzug) Auskunftspflichten bestehen. Hier wird verkannt, dass es auch beim RBB Vorgänge geben dürfte, die die grundrechtlich geschützte Freiheit der Berichterstattung[261] nicht tangieren. Das betrifft zum Beispiel Verträge des RBB über die Gebäudereinigung, die Beschaffung von Sachmitteln oder etwa Verträge mit Energieversorgern. Aus welchem Grund dieser wirtschaftlich-administrative Bereich dem Anwendungsbereich des IFG von vornherein entzogen sein sollte, ist – auch unter

258 Entschließung vom 24. Juni 2010: Informationsfreiheit bei öffentlich-rechtlichen Rundfunkanstalten, vgl. Dokumentenband 2010, S. 16

259 § 55 a WDR-Gesetz

260 Vgl. JB 2005, 6.2 (S. 203 f.)

261 Art. 5 Abs. 1 Satz 2 GG

Berücksichtigung des für den öffentlich-rechtlichen Rundfunk wesentlichen Strukturmerkmals der Staatsferne – nicht nachzuvollziehen.

Im zweiten Halbjahr tagte die IFK turnusgemäß unter dem Vorsitz der brandenburgischen Landesbeauftragten für das Recht auf Akteneinsicht. Auch vor dem Hintergrund der Veröffentlichung ausgewählter US-Botschaftsdepeschen durch WikiLeaks forderte die IFK öffentliche Stellen dazu auf, von sich aus **Initiativen für mehr Transparenz** zu ergreifen.[262] Zwar würden viele Behörden umfangreiche Informationen im Internet bereitstellen; allerdings sollten diese Aktivitäten gebündelt und über Internetplattformen – und damit auf einer breiteren Grundlage – für jedermann leicht zugänglich sein. In einer weiteren Entschließung appellierte die IFK an die Gesetzgeber, Rechtsgrundlagen für die **Offenlegung von Verträgen** zwischen der öffentlichen Hand und Unternehmen zu schaffen.[263] Diese Forderung ist deshalb besonders wichtig, weil sich öffentliche Stellen bei der Wahrnehmung ihrer Aufgaben zunehmend privater Unternehmen bedienen. Das betrifft auch zentrale Felder der staatlichen Daseinsvorsorge. Deshalb hielt die Konferenz es für zwingend geboten, den Zugang zu solchen Verträgen in den Informationsfreiheitsgesetzen sicherzustellen, wie dies beispielgebend jüngst im Berliner Informationsfreiheitsgesetz geschehen ist.

In der Tat war „Stein des Anstoßes" für diese Entschließung die Entwicklung in Berlin, an deren Ende die E**rgänzung des Berliner IFG** um Sonderregelungen insbesondere für Verträge der öffentlichen Grundversorgung stand.[264] Für diese im neuen § 7a IFG aufgezählten besonderen Verträge ist der Informationszugang im Vergleich zu anderen Verträgen erheblich erleichtert, denn die Offenbarung von Betriebs- und Geschäftsgeheimnissen allein kann die Offenlegung nicht verhindern. Zusätzlich muss dem Vertragspartner durch die Offenlegung ein wesentlicher wirtschaftlicher Schaden entstehen. Selbst in diesem Fall muss allerdings noch eine Abwägung getroffen werden: Überwiegt das Informationsinteresse das Geheimhaltungsinteresse, muss der Vertrag gleichwohl offengelegt werden. Neu ist auch die Pflicht zur Veröffentlichung solcher Grundversorgungsverträge; vor einer Entscheidung hierüber ist uns die Gelegenheit zur Stellungnahme zu geben.[265] Die Senatsverwaltung für Inneres und Sport hat ein erläuterndes Rundschreiben herausgegeben.[266]

262 Entschließung vom 13. Dezember 2010: Open Data: Mehr statt weniger Transparenz!, vgl. Dokumentenband 2010, S. 169
263 Entschließung vom 13. Dezember 2010: Verträge zwischen Staat und Unternehmen offen legen!, Dokumentenband 2010, S. 169
264 GVBl. vom 22. Juli 2010, S. 358

Die **Vorgeschichte** dieser bemerkenswerten Gesetzesnovelle beginnt 1999 mit der Teilprivatisierung der Anstalt des öffentlichen Rechts „Berliner Wasserbetriebe".[267] In dem Konsortialvertrag vereinbarte das Land Berlin mit den Investoren „absolutes Stillschweigen" über den Inhalt. 2007 verlangte ein Mitglied des Abgeordnetenhauses vom Senat Einblick in sämtliche Akten in Zusammenhang mit der Teilprivatisierung der Wasserbetriebe einschließlich des Konsortialvertrages. Nach teilweiser Ablehnung dieses Begehrens durch den Senat erhob die Abgeordnete Klage vor dem Verfassungsgerichtshof unter Berufung auf ihr verfassungsrechtlich gewährleistetes Akteneinsichtsrecht.[268] Der Verfassungsgerichtshof gab ihr Recht:[269] Der Senat habe die partielle Verweigerung der Akteneinsicht lediglich pauschal und formelhaft und nicht bezogen auf einzelne Unterlagen begründet. Auch könne die vertraglich vereinbarte Geheimhaltung der Abgeordneten nicht entgegengehalten werden, denn sie stehe unter dem ausdrücklichen Vorbehalt, dass gesetzliche Vorschriften nicht zur Offenlegung verpflichteten.

Als maßgeblich für die Gesetzesänderung kann die **Bürgerinitiative „Berliner Wassertisch"**, Trägerin des Volksbegehrens „Schluss mit Geheimverträgen – Wir Berliner wollen unser Wasser zurück!", angesehen werden. Es zielte auf die vorbehaltlose Offenlegung der Verträge mit privatrechtlichen und öffentlich-rechtlichen Wasserversorgungsunternehmen.[270] Obwohl ihrem Anliegen durch die Änderung des IFG weitgehend Rechnung getragen und der Vertrag zur Teilprivatisierung der Berliner Wasserbetriebe mit sämtlichen Anlagen und allen späteren Änderungsvereinbarungen vom Senat im Internet auf Grund des neuen § 17 Abs. 3 Satz 1 IFG veröffentlicht wurde,[271] trieb die Bürgerinitiative das Volksbegehren weiter voran, um weitere Forderungen wie die rück-

265 § 17 Abs. 3 IFG
266 Rundschreiben I Nr. 64/2010 vom 23. November 2010
267 Vgl. dazu insgesamt A. Dix: Aktive Transparenz bei Grundversorgungsverträgen – Das Berliner Modell. In: Informationsfreiheit und Informationsrecht, Jahrbuch 2010, S. 133 ff.
268 Art. 45 Abs. 2 Verfassung von Berlin (VvB)
269 Urteil vom 14. Juli 2010 – VerfGH 57/08
270 JB 2009, 14.2.1
271 Bekanntmachung vom 25. November 2010, ABl. Nr. 50 vom 10. Dezember 2010, S. 1985

wirkende Nichtigkeit von nicht veröffentlichten Verträgen durchzusetzen. Der am 13. Februar 2011 durchgeführte Volksentscheid war erfolgreich.

Der EuGH hat die vollständige **Veröffentlichung von EU-Agrarsubventionen** und ihrer Empfänger im Internet gestoppt[272] und damit zwei Landwirten aus Hessen im Ergebnis Recht gegeben. Zwar verfolge die zugrunde liegende EU-Verordnung ein legitimes Ziel, weil die vorgeschriebene Transparenz den Bürgerinnen und Bürgern eine Beteiligung an der öffentlichen Debatte über die Verwendung der Mittel aus dem EU-Landwirtschaftsfonds ermögliche. Allerdings habe der europäische Gesetzgeber bei der Anordnung der pauschalen Veröffentlichungspflicht unzulässig in das Privatleben der Subventionsempfänger eingegriffen. Die Auflistung der Empfängernamen und der genauen Beträge sei im Hinblick auf das Ziel der Transparenz unverhältnismäßig, da keine Gewichtung nach Art, Häufigkeit und Umfang der Beihilfen vorgenommen worden sei. Bezüglich juristischer Personen ist jedoch die Veröffentlichung weiterhin uneingeschränkt zulässig. Gleichwohl hat die Bundesregierung sie in Abstimmung mit der Europäischen Kommission insgesamt ausgesetzt.[273] Beide verkennen, dass der Gerichtshof eine differenzierte Veröffentlichung der Namen von Subventionsempfängern, auch soweit es sich um natürliche Personen handelt, als zulässig angesehen hat, wenn dabei die Höhe und die Bezugsdauer der Subvention berücksichtigt werden.

Im Mai hat die Bundesregierung den Bericht über die Ergebnisse der **Evaluation des Verbraucherinformationsgesetzes (VIG)** veröffentlicht.[274] Darin wird festgestellt, dass sich das VIG grundsätzlich bewährt habe, unter diversen Aspekten allerdings optimierungsbedürftig sei. Der Öffentlichkeit wurde Gelegenheit zur Stellungnahme gegeben.[275] Hiervon hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) Gebrauch gemacht und erneut einen direkten Informationsanspruch gegenüber Unternehmen ebenso gefordert wie die Zusammenführung der Vorschriften des IFG, UIG und VIG in einem einheitlichen Gesetz auf Bundesebene, welches dann als Vorbild für

272 Urteil vom 9. November 2010, Rs. C-92/09 und C-93/09; vgl. JB 2008, 15.1 (S. 168)
273 BT-Drs. 17/3807, S. 58 f. (Antwort der Bundesregierung auf die Frage der Abgeordneten Dr. Tackmann)
274 BT-Drs. 17/1800
275 www.vigwirkt.de

die Landesgesetzgebung dienen kann.[276] Auch wird für eine proaktive Information der Öffentlichkeit bei der Lebensmittelkontrolle plädiert und dabei auf die Erfahrungen des **Smiley-Projekts** in Pankow verwiesen, die belegen, *„dass die Veröffentlichung positiver Kontrollergebnisse – im Gegensatz zur Beschränkung auf Verstöße – die Akzeptanz der betroffenen Unternehmen stärkt, da sie die eigene Regeltreue zu Werbungszwecken nutzen können“.*

Dieses **Berliner Modellprojekt**[277] erhielt bundesweiten Rückenwind durch die Verbraucherschutzministerkonferenz, die im September die Einführung eines einheitlichen Systems zur Transparenz in der Lebensmittelüberwachung beschlossen hat. Kurz darauf entschieden auch die Bezirke mit der zuständigen Senatsverwaltung, in Berlin zum 1. Juli 2011 ein einheitliches Smiley-System nach dänischem Vorbild einzuführen. Eine Negativliste mit Fotos, wie sie im Pankower Modellprojekt geführt wird, soll es dann nicht mehr geben. Außerdem hat der Senat eine entsprechende Bundesratsinitiative beschlossen.

Nach wie vor wird in Berlin über mehr Transparenz beim **Sponsoring** diskutiert.[278] Dabei wäre schon viel erreicht, wenn es einheitliche Vorschriften für alle öffentlichen Stellen gäbe,[279] wie es in anderen Bundesländern der Fall ist.[280]

14.2 Einzelfälle

„Zöllner stoppt CDU-Umfrage zum Lehrermangel“

So lautete der Titel einer Zeitungsmeldung[281], nach der die Bildungsverwaltung den Schulen die Teilnahme an der Umfrage eines Abgeordneten zum Lehrermangel untersagt hatte. Begründet wurde das damit, dass Abgeordnete zwar nach der Verfassung von Berlin ein umfassendes Auskunfts- und Akteneinsichtsrecht gegenüber dem Senat hätten, nicht aber gegenüber jedem Mitarbeiter oder jeder Schule.

276 Stellungnahme vom 2. September 2010, vgl. Dokumentenband 2010, S. 156
277 JB 2008, 15.2.2
278 JB 2009, 14.2.1 (a. E.)
279 Vgl. Antrag der Fraktion Bündnis 90/Die Grünen, Abgh-Drs. 16/3449
280 So z. B. in Hamburg, Mecklenburg-Vorpommern und Sachsen-Anhalt
281 Der Tagesspiegel vom 30. September 2010, S. 12

Diese Auffassung berücksichtigte nicht, dass sich Abgeordnete bei einem Informationszugangsbegehren gegenüber der Verwaltung nicht nur auf Art. 45 VvB berufen können, sondern daneben auf das IFG. Nach dessen § 3 Abs. 1 hat nämlich grundsätzlich jeder Mensch einen Anspruch auf Zugang zu den bei öffentlichen Stellen des Landes Berlin – also auch bei öffentlichen Schulen – vorhandenen Informationen. Aus welchem Grund ein Informationsrecht über die Frage, wie viel Personal zahlenmäßig an der jeweiligen Schule fehlt, eingeschränkt oder sogar ausgeschlossen sein sollte,[282] war nicht ersichtlich. Dies haben wir der Bildungsverwaltung mitgeteilt. Sie stimmte zwar der Auffassung zu, dass grundsätzlich auch Abgeordneten Ansprüche nach dem IFG zustehen. Im vorliegenden Fall habe sich der Abgeordnete allerdings nicht auf diese Rechtsgrundlage berufen. Hierbei hat die Bildungsverwaltung jedoch verkannt, dass bei Ansprüchen gegen den Staat die Rechtsgrundlage nicht konkret benannt werden muss. Vielmehr obliegt es dem Staat selbst, den Anspruch unter allen in Frage kommenden Gesichtspunkten zu prüfen.

Niemand muss einer Behörde die konkrete Anspruchsgrundlage für ein Informationszugangsbegehren nennen. Es kann vom Staat erwartet werden, dass er Informationszugangsansprüche unter Würdigung aller in Betracht kommenden Rechtsgrundlagen prüft, die er selbst am besten kennen müsste.

Dienstaufsichtsbeschwerde beim Polizeipräsidenten

Ein Bürger beschwerte sich beim Polizeipräsidenten über einen Mitarbeiter und verlangte später Informationen über die veranlassten Maßnahmen und den Ausgang der Dienstaufsichtsbeschwerde. Wir wurden gefragt, welche Rechtsgrundlage für das Informationszugangsbegehren gelte.

Da Dienstaufsichtsbeschwerde-Vorgänge zur Personalakte im materiellen Sinne gehören, gilt primär weder das Berliner Datenschutzgesetz noch das IFG noch das Berliner Verwaltungsverfahrensgesetz, sondern das speziellere Personalaktendatenschutzrecht des Landesbeamtengesetzes (LBG).[283] Es regelt

282 § 5 ff. IFG
283 § 84 ff. LBG (entsprechend anwendbar auf Angestellte); vgl. VG Berlin, Beschluss vom 18. März 2010 – VG 2 K 5.09

detailliert, wer im Einzelnen Zugang zur Personalakte hat. Dazu gehören auch Dritte, also auch Dienstaufsichtsbeschwerdeführer. Sie haben unter den engen gesetzlichen Voraussetzungen ein Recht auf Auskunft, jedoch kein Recht auf Akteneinsicht.[284]

Für den Informationszugang zu Dienstaufsichtsbeschwerde-Vorgängen gilt ausschließlich das speziellere Personalaktendatenschutzrecht.

Kfz-Schaden und Ast-Bruch in Charlottenburg–Wilmersdorf

Ein Rechtsanwalt beschwerte sich darüber, dass ihm die Einsicht in einen Schadensvorgang im Bezirksamt Charlottenburg–Wilmersdorf versagt wurde. Ein abgebrochener Ast habe den Pkw seiner Mandantin beschädigt. Zur Prüfung der Erfolgsaussichten eines Schadensersatzanspruchs habe er Nachweise über die 2009 durchgeführten Baumkontrollen verlangt. Das Bezirksamt begründete die Ablehnung mit § 9 Abs. 1 Satz 1 IFG, weil nach der besonderen Art der Verwaltungstätigkeit ein Bekanntwerden des Akteninhalts mit einer ordnungsgemäßen Aufgabenerfüllung unvereinbar sei. Dies ergebe sich daraus, dass der Rechtsanwalt einen zivilrechtlichen Schadensersatzanspruch gegen das Land Berlin geltend mache. Dem im Zivilrecht herrschenden Prinzip der Gleichrangigkeit von Klägerin und Beklagtem würde es widersprechen, wie im öffentlichen Recht direkt Akteneinsicht zu gewähren.

Wir haben dem Bezirksamt mitgeteilt, dass die Berufung auf § 9 Abs. 1 Satz 1 IFG rechtsfehlerhaft ist. Dass ein Schadensersatzprozess droht, ist kein Ablehnungsgrund, wie aus dem bereits seit 2006 geltenden § 9 Abs. 1 Satz 2 IFG im Umkehrschluss hervorgeht. Danach kann die Akteneinsicht allenfalls bei laufenden Gerichtsverfahren und nur bei nachteiligen Auswirkungen für das Land Berlin versagt werden. Leider hat sich das Bezirksamt diesem Hinweis verschlossen und dem Widerspruch nicht abgeholfen. Das (vermeidbare, monatelange) gerichtliche Verfahren endete zugunsten der Bürgerin.[285]

284 § 88 Abs. 2 LBG
285 VG Berlin, Urteil vom 7. Oktober 2010 – VG 2 K 71.10

Die Tatsache, dass ein Gerichtsverfahren droht, ist kein Grund, den Informationszugang zu Schadensvorgängen zu verweigern.

Aus der Praxis

BVV-Sitzungen im Internet

Das Bezirksamt Marzahn–Hellersdorf bat uns um Prüfung, ob Bedenken gegen die Übertragung öffentlicher BVV-Sitzungen im Internet bestünden. Insbesondere sei fraglich, ob alle Bezirksverordneten zustimmen müssen oder ob ein einstimmig oder mehrheitlich gefasster BVV-Beschluss ausreicht. Das Bezirksamt hielt die jeweilige Zustimmung für erforderlich.

Diese Auffassung war zutreffend. Die Live-Übertragung der BVV-Sitzungen (in Bild und Ton) im Internet mag eine Maßnahme sein, die das „gläserne" Rathaus fördert und damit im Sinne der Informationsfreiheit ist. Da es für diese „weltweite" Datenübermittlung aber keine Rechtsgrundlage gibt, ist sie nur mit Einwilligung aller Betroffenen zulässig. Ein mehrheitlich gefasster BVV-Beschluss reicht nur dann aus, wenn ein betroffenes BVV-Mitglied die Möglichkeit hat, sich dem zu entziehen, z. B. indem der Live-Stream für die Dauer der Rede ausgeschaltet wird. BVV-Mitglieder, die ganz grundsätzlich eine Übertragung ihrer Bilder und Worte ins Internet ablehnen, können dies einmalig für alle künftigen BVV-Sitzungen erklären. Das sollte dokumentiert, also schriftlich festgehalten werden, auch damit eine dauerhafte Beachtung dieses Willens durch die Sitzungsleitung sichergestellt ist. Andere Personen wie Besucher und Bezirksamtsmitglieder, die von Bild-/Tonübertragungen im Internet betroffen sind, müssen vor jeder BVV-Sitzung um ihre Einwilligung gebeten werden.

Aus der Praxis

Transparenz bei Bezirksverordneten in Treptow–Köpenick

Ein Bezirksverordneter bat uns um Prüfung, ob es Bedenken gegen die geplante Umsetzung eines BVV-Beschlusses gebe. Darin würden BVV-Mitglieder, die Bürgerdeputierten und Mitglieder des Bezirksamtes aufgefordert, Angaben über ihre vergüteten oder ehrenamtlichen Funktionen in Verbänden, Vereinen, Beiräten, Genossenschaften, Stiftungen, Aufsichtsräten sowie Projekten freier und öffentlicher Träger dem BVV-Büro bekannt zu geben. Auch soll die unselbstständige oder selbstständige berufliche Tätigkeit angegeben werden. Mit einem Fragebogen sollten die Daten der Betroffenen erhoben und im Internetangebot der BVV veröffentlicht werden.

Vor dem Hintergrund des Informationsfreiheitsgedankens und der Überprüfbarkeit des Handelns der öffentlichen Verwaltung durch die Bürgerinnen und Bürger begrüßen wir solche Bemühungen um mehr Transparenz grundsätzlich sehr. Allerdings – so haben wir mitgeteilt – wäre eine Veröffentlichung weder vom BlnDSG noch vom IFG gedeckt gewesen. Eine besondere Rechtsvorschrift, die eine Veröffentlichung der Daten erlaubt, muss den Anforderungen von § 6 Abs. 1 Satz 3 BlnDSG genügen, d. h. einen diesem Gesetz vergleichbaren Datenschutz gewährleisten. Eine solche Rechtsvorschrift ist aber weder im Bezirksverwaltungsgesetz noch in der Geschäftsordnung der BVV enthalten. Eine Veröffentlichung der Angaben im Internet stellt eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs dar und ist nach § 13 BlnDSG ohne Erlaubnistatbestand nur zulässig, wenn der Betroffene eingewilligt hat. Die Voraussetzungen für eine wirksame Einwilligung lagen hier nicht vor. Weder existierte ein schriftlicher Einwilligungstext noch war die Freiwilligkeit der Einwilligung sichergestellt. Ein generelles Recht bzw. eine Pflicht, Informationen, die auch personenbezogene Daten enthalten, von sich aus zu veröffentlichen, statuiert das IFG nicht.

Schließlich war noch Folgendes zu berücksichtigen: Selbst bei Mitgliedern des Bundestages, für die als Teil der Legislative und als Repräsentanten des gesamten Volkes zur Absicherung der Freiheit der Mandatsausübung vor äußeren Einflüssen gewiss noch andere Maßstäbe anzulegen sind, wurde in der zu § 44a Abgeordnetengesetz ergangenen Entscheidung des Bundesverfassungsgerichts kontrovers erörtert, ob das Recht auf informationelle Selbstbestimmung einer Veröffentlichung entgegensteht.[286] Für die Mitglieder der BVV wie auch des Bezirksamts ist dies zweifelsohne der Fall. Die BVV ist kein Parlament, sondern (wie das Bezirksamt) ein Organ der bezirklichen Selbstverwaltung.[287]

Beide Fälle zeigen, dass auch Bezirksverordnete ein Recht auf informationelle Selbstbestimmung haben, insbesondere weil einmal Veröffentlichtes aus dem Internet nicht mehr „zurückgeholt" werden kann.

286 Urteil vom 4. Juli 2007 – 2 BvE 1/06; 2 BvE 2/06; 2 BvE 3/06; 2 BvE 4/06, BVerfGE 118, Rn. 277 ff.

287 Art. 72 Abs. 1 VvB, § 2 BezVG

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

Eine Bürgerin beschwerte sich über ihren Versicherungsmakler, der ihr einen **„Fragebogen für den Abgleich ihrer persönlichen Daten“** zuleitete. Dabei waren Fragen zu Haus- und Grundbesitz, Hausrat, Haustieren, Land- und Wasserfahrzeugen. Warum die Daten erhoben wurden, ergab sich aus dem Anschreiben nicht. Der Versicherungsmakler teilte uns mit, er sei in dieser Funktion verpflichtet festzustellen, ob in einem Bereich eine **Unterversicherung** besteht. Wir haben durchgesetzt, dass er seine Kundinnen und Kunden zukünftig darauf hinweist, dass die Preisgabe der personenbezogenen Daten freiwillig erfolgt. Außerdem wird er die Zweckbestimmung der Datenerhebung genauer erläutern.

Eine Bank kündigte nach 29 Jahren die Geschäftsbeziehung zu einem Kunden. Auf Nachfrage teilte sie ihm mit, sie sei nach den Allgemeinen Geschäftsbedingungen nicht verpflichtet, die Beendigung der Geschäftsbeziehung zu begründen. Die Kündigung war von der Abteilung **Geldwäscheprävention** der Bank veranlasst worden. Bei Auftreten eines Verdachts weist diese Abteilung die zuständigen Kundenberaterinnen und -berater an, das betroffene Konto zu schließen. Ihnen wurde dabei nur die Kontonummer des verdächtigen Kontos mitgeteilt. Die Kontokündigung des Betroffenen erfolgte versehentlich, da der Abteilung Geldwäscheprävention ein verhängnisvoller **Zahlendreher** bei der Kontonummer unterlaufen war. Um zukünftig ähnliche Fehler zu vermeiden, wurde das Verfahren der Kündigungsanordnung präzisiert. Diese enthält nun neben der Kontonummer den Namen und die Anschrift der Kontoinhaberin oder des Kontoinhabers.

Eine Empfängerin von Leistungen nach dem SGB II musste sich zur Feststellung ihrer Erwerbsfähigkeit einer ärztlichen Untersuchung unterziehen. Eine Vertragsärztin der Bundesagentur für Arbeit hat deshalb ein medizinisches Gutachten erstellt. Der für das Berliner Jobcenter bestimmte und diesem auch zugegangene Gutachtenteil enthielt konkrete **medizinische Diagnosen.**

Diese Datenübermittlung war unzulässig, da die Kenntnis der konkreten Diagnosen für die arbeitsmedizinische Beurteilung nicht erforderlich war. Vollkommen ausreichend ist, dass die Beschwerden benannt werden. Dies haben wir dem medizinischen Dienst der Bundesagentur mitgeteilt. Daraufhin ist ein neues Gutachten erstellt worden; zudem hat der medizinische Dienst das Jobcenter über die Ungültigkeit des ursprünglichen Gutachtens informiert.

Im Rahmen eines unterrichtsergänzenden Bildungsangebots (einer **Bastelveranstaltung für Kinder**), das vom Europäischen Sozialfonds (ESF) mitfinanziert wurde, wurden die Eltern aufgefordert, Namen, Vornamen, Adresse, Geschlecht, Staatsangehörigkeit und Geburtsdatum ihrer Kinder gegenüber dem Veranstalter anzugeben. Zur Begründung wurde angeführt, die Europäische Union fordere eine lückenlose Auflistung aller an ESF-Maßnahmen Teilnehmenden. Auf Nachfrage teilte uns die zuständige Senatsverwaltung für Wirtschaft, Technologie und Frauen mit, dass das Bastelangebot versehentlich als Qualifizierungsmaßnahme im Rahmen des Gesamtprojekts klassifiziert worden sei, bei der die Erhebung der Daten tatsächlich wegen der Nachweisführung gegenüber dem ESF erforderlich gewesen wäre. Die Senatsverwaltung teilte unsere Auffassung, dass die Daten für das Bastelangebot selbst in dem erhobenen Umfang nicht notwendig waren. Wir haben einen datenschutzrechtlichen Mangel festgestellt. Da die Senatsverwaltung zugesagt hat, dass sich die rechtswidrige Praxis nicht wiederholen wird, haben wir von weiteren Maßnahmen abgesehen.

Um Kundinnen und Kunden auch telefonisch ohne ausdrückliche Einwilligung bewerben zu können, rief ein Unternehmen sie zunächst an. In dem Gespräch bat das Unternehmen lediglich um die Einwilligung, zukünftig den Betroffenen weitere interessante Angebote zum Unternehmen telefonisch unterbreiten zu dürfen. Auch ein Telefonat, in dem ein Unternehmen um eine Einwilligung in die telefonische Ansprache bittet, stellt Werbung dar. Der Anruf selbst dient nämlich der **Ankündigung von Werbung** und der Nennung des werbenden Unternehmens. Soweit Verbraucherinnen und Verbraucher in diese Werbeform nicht vorher ausdrücklich eingewilligt haben, liegt wegen der damit einhergehenden unzumutbaren Belästigung ein wettbewerbswidriger Eingriff vor (**Cold Calling**)[288]. Die Telefonnummer wurde ursprünglich für Vertragszwecke verarbeitet. Die vorgenommene Zweckänderung ist nur in den gesetz-

288 § 7 Abs. 1 und 2 Nr. 2 UWG; vgl. JB 2008, 2.1

lichen Ausnahmefällen möglich, die aber hier nicht vorlagen. Eine Einwilligung per Telefon entspricht auch nicht den Formanforderungen des Bundesdatenschutzgesetzes: Sie ist grundsätzlich nur wirksam, wenn sie schriftlich erteilt wird. Das Unternehmen hat nach unserer Aufforderung die rechtswidrige Praxis der telefonischen Abfrage von Einwilligungen eingestellt.

Ein Rechtsanwalt beschwerte sich darüber, dass er vom IT-Dienstleistungszentrum (ITDZ) keine Antwort auf die Frage erhalten habe, in welchem Verhältnis **Führungspositionen** beim ITDZ d**urch Männer und Frauen besetzt** sind. Hintergrund war eine Auseinandersetzung um eine Ein-/Höhergruppierung einer Beschäftigten. Nach unseren Interventionen erhielt der Rechtsanwalt die seit dem letzten Frauenförderplan aktualisierten Daten, sodass ein Prozess allein hierüber verhindert werden konnte.

Eine Bürgerin beschwerte sich darüber, dass das Bezirksamt Pankow ihr als Pächterin eines Grundstücks nicht mitteilen wollte, welche **Maßnahmen zur Einrichtung eines Abwasseranschlusses** gegen die Wohnungsbaugesellschaft als Eigentümerin des Grundstücks ergriffen wurden. Insbesondere wollte sie wissen, aus welchem Grund das Bezirksamt in den vergangenen Jahren nichts gegen die Eigentümerin unternommen hat. Nach Klärung des umfangreichen Sachverhalts konnten wir die Petentin davon überzeugen, dass die Gründe selbst sich nicht aus der Akte ergeben werden, wenn schlichte Untätigkeit des Bezirksamts vorliegt. Das Bezirksamt haben wir davon überzeugt, dass die uns mitgeteilte Tatsache, dass ein Verwaltungszwangsverfahren gegen die Wohnungsbaugesellschaft läuft, keine nach § 6 oder § 7 IFG schützenswerte Information und deshalb auch der Petentin mitzuteilen ist.

16. Aus der Dienststelle

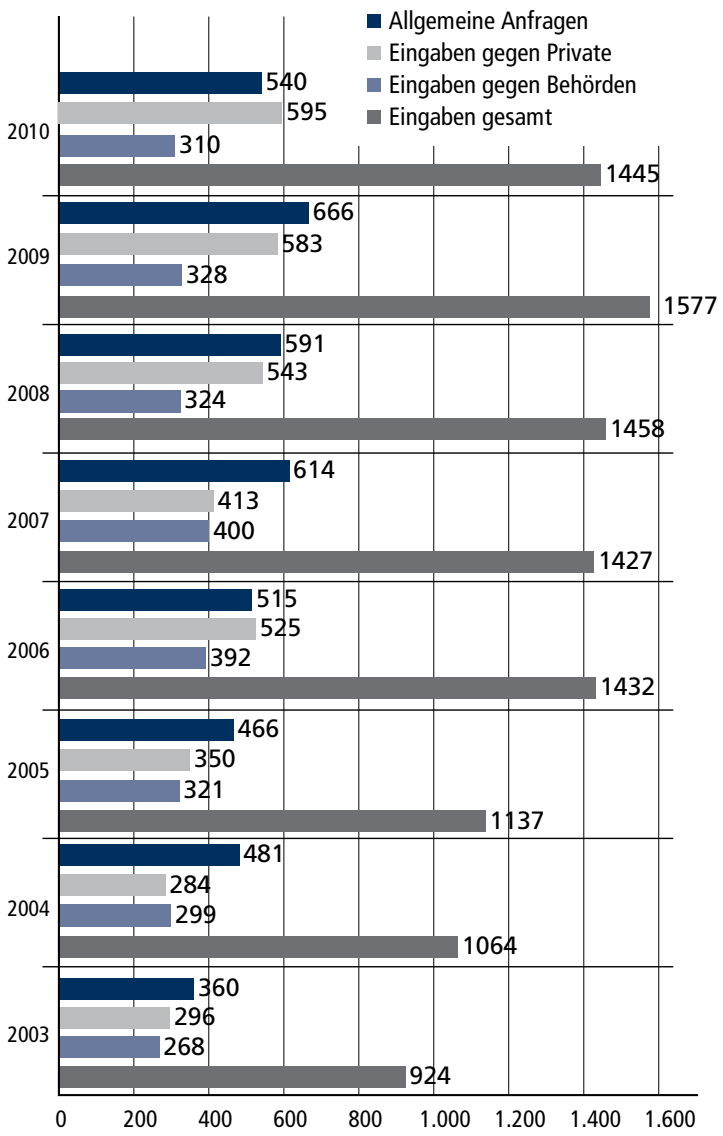
16.1 Entwicklungen

Im August verstarb unerwartet Dipl.-Volkswirt Dr. Rainer Metschke, der seit 1992 als Referent für Bildung, Wissenschaft und Statistik in der Dienststelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit tätig war. Dr. Metschke war auch außerhalb Berlins als engagierter Fachmann anerkannt und für zahlreiche Wissenschaftler an den Berliner Hochschulen stets ein kompetenter Ansprechpartner. Sein Tod war ein herber Verlust für die Dienststelle.

Die Neuorganisation des juristischen Bereichs der Dienststelle[289] hat sich bewährt. Die beiden Bereiche Recht I und Recht II mit der Sanktionsstelle sowie der Servicestelle Bürgereingaben (früher BürgerOffice) können den gestiegenen Beratungsbedarf der Öffentlichkeit, von Behörden und Unternehmen besser befriedigen. Gleichwohl wachsen sowohl der Problemdruck durch technische Entwicklungen mit Risiken für den Datenschutz als auch der Bedarf an Vor-Ort-Kontrollen weiter.

Die Zahl der Eingaben, die sich gegen öffentliche Stellen richten, ist in den zurückliegenden acht Jahren nahezu identisch geblieben, während die Eingaben gegen private Datenverarbeiter in den letzten vier Jahren permanent zugenommen haben.[290] Zugleich setzten wir im Berichtszeitraum wegen Verstößen gegen das Bundesdatenschutzgesetz Bußgelder in Höhe von insgesamt 52.120,- Euro fest, wovon Bußgeldbescheide über 35.120,- Euro bisher Rechtskraft erlangten.

289 JB 2009, 16.1
290 Vgl. Grafik nächste Seite



Anzahl der Bürgereingaben im Jahresvergleich 2003–2010

16.2 Zusammenarbeit mit dem Abgeordnetenhaus

Im Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses sind der Jahresbericht 2008 und die Stellungnahme des Senats[291] beraten und mit Beschlussempfehlungen versehen worden. Diese Empfehlungen hat das Abgeordnetenhaus am 17. Juni angenommen.[292] Das Landesparlament folgt mit diesem Verfahren seit langem dem Beispiel des Deutschen Bundestages, der ebenfalls die Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Anlass für Beschlüsse nimmt, in denen die Verwaltung wie auch die Wirtschaft auf verbesserungsbedürftige Bereiche – insbesondere beim Datenschutz – hingewiesen wird. Zugleich wurden im Unterausschuss „Datenschutz und Informationsfreiheit“ Gesetzgebungsvorhaben (z. B. die weitreichende Änderung des Berliner Informationsfreiheitsgesetzes[293]) parteiübergreifend konstruktiv behandelt.

16.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** tagte am 17./18. März in Stuttgart und am 3./4. November in Freiburg unter dem Vorsitz des Landesbeauftragten für den Datenschutz Baden-Württemberg. Dabei fasste sie zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[294] Für 2011 hat der Bayerische Landesbeauftragte für den Datenschutz den Konferenzvorsitz übernommen.

Die im **Düsseldorfer Kreis** kooperierenden Aufsichtsbehörden für den **Datenschutz in der Privatwirtschaft** haben unter dem Vorsitz des niedersächsischen Datenschutzbeauftragten am 28./29. April in Hannover und unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen am 24./25. November in Düsseldorf getagt und jeweils Entschlie-

291 Abgh.-Drs. 16/2576
292 Vgl. Anhang 1
293 Vgl. 14.1
294 Vgl. Dokumentenband 2010, S. 9

ßungen zu zahlreichen Fragen des Datenschutzes im Bereich der Wirtschaft gefasst.[295] Für 2011 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen weiterhin den Vorsitz.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 24. Juni unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit in Berlin und am 13. Dezember in Kleinmachnow unter dem Vorsitz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg. Die Konferenz fasste Entschließungen zu öffentlich-rechtlichen Rundfunkanstalten, zu Open Data und zur Offenlegung von Verträgen.[296] Für das erste Halbjahr 2011 hat die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen den Vorsitz dieser Konferenz übernommen.

Auf europäischer Ebene vertritt seit jeher Berlin die Bundesländer im Auftrag der Konferenz der Datenschutzbeauftragten und der Aufsichtsbehörden in der **Arbeitsgruppe nach Artikel 29 der Europäischen Datenschutzrichtlinie.** Die Gruppe hat wieder wichtige Arbeitspapiere und Stellungnahmen verfasst.[297] Auf Einladung der tschechischen Datenschutzbehörde fand die **Europäische Konferenz der Datenschutzbeauftragten** am 29./30. April in Prag statt. Sie fasste Entschließungen zum Einsatz von Körperscannern an Flughäfen und zu dem geplanten Abkommen zwischen der Europäischen Union und den USA über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.[298] Unter dem Vorsitz der israelischen Datenschutzbehörde fand die **32. Internationale Konferenz der Datenschutzbeauftragten** vom 27.–29. Oktober in Jerusalem statt. Dem ging eine zweitägige Konferenz der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zum 30-jährigen Jubiläum der Verabschiedung der Datenschutzrichtlinien dieser Organisation voraus, die als erste internationale Organisation weltweite Datenschutzprinzipien formuliert hatte. Die OECD diskutiert gegenwärtig – ebenso wie die Gremien der Europäischen Union und der Europarat – über die notwendigen Veränderungen dieser Prinzipien angesichts der Herausforderungen des 21. Jahrhunderts.

295 Vgl. Dokumentenband 2010, S. 22
296 Vgl. 14.1
297 Vgl. 11.1 (a. E.)
298 Vgl. Dokumentenband 2010, S. 30

Die **Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group")** tagte unter unserem Vorsitz am 15./16. April in Granada und am 6./7. September in Berlin. Die Gruppe verabschiedete die „‚Granada Charta' des Datenschutzes in einer digitalen Welt" sowie mehrere Arbeitspapiere.[299] Schließlich ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit dem **Global Privacy Enforcement Network (GPEN – Globales Netz zur Durchsetzung des Datenschutzes)**[300] beigetreten, das auf Initiative der U.S. Federal Trade Commission ins Leben gerufen wurde. Diesem Netz von Datenschutzbehörden gehören außerdem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Datenschutzbehörden aus Australien (Bundesbeauftragter und die Beauftragten der Staaten Queensland und Victoria), Bulgarien, Frankreich, Großbritannien, Guernsey, Irland, Israel, Italien, Kanada, Neuseeland, Niederlande, Polen, Schweiz, Slowenien, Spanien und Tschechien an. Ziel dieses Netzwerkes ist es, sich über Durchsetzungsmethoden und -strategien zu informieren, was gerade angesichts der weltweit agierenden Datenverarbeiter etwa im Internet von großer praktischer Bedeutung ist.

299 Vgl. 13.3
300 www.privacyenforcement.net

16.4 Öffentlichkeitsarbeit

Am 28. Januar fand zum Thema „Gesundheitsdaten im Netz – Zu Risiken und Nebenwirkungen für das Persönlichkeitsrecht der Patienten“ im Hufeland-Hörsaal der Charité der 4. Europäische Datenschutztag statt.

Am 4. Oktober haben die Datenschutzbeauftragten des Bundes und der Länder ein Symposium zum Thema „Modernes Datenschutzrecht für das 21. Jahrhundert“ im Abgeordnetenhaus veranstaltet.

Außerdem beteiligten wir uns an folgenden öffentlichen Veranstaltungen:

- Tag der offenen Tür im Abgeordnetenhaus am 29. Mai
- 6. Jugendverbraucherschutztag im Freizeit- und Erholungszentrum Wuhlheide am 29. September
- Jugendmesse YOU am 1./2. Oktober.

Darüber hinaus haben wir an zahlreichen Veranstaltungen insbesondere zum Thema Kinder- und Jugendschutz teilgenommen.[301]

Berlin, den 30. März 2011

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

301 Vgl. 8.1.4

Anhänge

Beschlüsse des Abgeordnetenhauses vom 17. Juni 2010

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2008

1. Datenverarbeitung in der Berliner Verwaltung hier: IT-Politik für die Berliner Verwaltung, IT-Sicherheit in Berlin (1.2.1, 1.2.2, Drs S. 10 ff)

Der Senat wird aufgefordert, dafür zu sorgen, dass unter Berücksichtigung der Erfahrungen des Polizeipräsidenten in Berlin und beginnend in den Behörden, die besonders umfangreiche und komplexe informationstechnische Systeme und Verfahren betreiben, ein IT-Sicherheitsmanagement eingerichtet wird, damit nicht nur die einmalige Erstellung von Sicherheitskonzepten, sondern auch deren nachhaltige Anpassung an geänderte technische, organisatorische und personelle Umgebungen sowie neu bekannt werdende Risiken organisatorisch sichergestellt werden.

2. Kontrolle der IT-Sicherheit beim polizeilichen Informationssystem POLIKS (3.2, Drs S. 40 ff)

Der Senat wird aufgefordert, dafür zu sorgen, dass unter Berücksichtigung der Erfahrungen des Polizeipräsidenten in Berlin und beginnend in den Behörden, die besonders umfangreiche und komplexe informationstechnische Systeme und Verfahren betreiben, ein IT-Sicherheitsmanagement eingerichtet wird, damit nicht nur die einmalige Erstellung von Sicherheitskonzepten, sondern auch deren nachhaltige Anpassung an geänderte technische, organisatorische und personelle Umgebungen sowie neu bekannt werdende Risiken organisatorisch sichergestellt werden.

3. Vorlage von Mietverträgen im Besteuerungsverfahren eines Vermieters (7.3, Drs S. 59 f.)

Der Senat wird aufgefordert, durch eine Dienstanweisung sicherzustellen, dass die Finanzverwaltung bei der Ermittlung der steuerpflichtigen Einkünfte eines Vermieters aus der Vermietung und Verpachtung personenbezogene Mieterdaten nur im jeweils erforderlichen Umfang erhebt. Steuerpflichtige sollten darauf hingewiesen werden, dass sie nicht erforderliche Angaben, z. B. in Mietverträgen, schwärzen dürfen.

4. Errichtung einer automatisierten Schülerdatei in Berlin (10.2.2, Drs S. 101 ff)

Der Senat wird aufgefordert sicherzustellen, dass das Thema „Datenschutz" künftig verstärkt in den Schulunterricht integriert wird. Der Schutz der Privatsphäre des Einzelnen ist eine schulische Bildungsaufgabe, die Eingang in die Lehrpläne finden muss.

5. Informationsfreiheit – Entwicklungen für und gegen mehr Transparenz hier: Mehr Transparenz bei Lobbyisten (15.1 Drs S. 137)

Der Senat wird aufgefordert, nach dem Vorbild der Bundesregierung jährlich über den Einsatz externer Personen und Gutachter in der Berliner Verwaltung (sog. Lobbyisten) zu berichten. Dieser Bericht ist allgemein zugänglich zu machen. Ferner wird geprüft, ob nach dem Vorbild der Europäischen Kommission ein sog. Lobbyisten-Register machbar ist.

6. Informationsfreiheit in Berlin – Allgemeine Entwicklungen hier: Offenlegung von Verträgen der öffentlichen Hand (15.2.1, Drs S. 140)

Der Senat wird aufgefordert, mit einem Schreiben an die öffentlichen Stellen des Landes Berlin darauf hinzuwirken, dass die öffentliche Hand – insbesondere im Bereich der Grundversorgung – künftig keine pauschale Vereinbarung mit dem Vertragspartner über die Geheimhaltung des gesamten Vertrages schließt und stattdessen im Vertrag auf das Berliner Informationsfreiheitsgesetz hinweist, nach dem auf Antrag eine (u. U. nur teilweise) Offenlegung des Vertrages in Betracht kommen kann.

7. Informationsfreiheit in Berlin / Allgemeine Entwicklungen hier: Internet-Portal für Verwaltungsvorschriften (15.2.1, Drs S. 140 f.)

Der Senat wird aufgefordert, dafür zu sorgen, dass die Berliner Verwaltung ein einheitliches Transparenz-Niveau dadurch schafft, dass sie Dienst- und Verwaltungsvorschriften, fachliche Weisungen u. Ä. über ein zentrales Internet-Portal allgemein zugänglich macht. Dem Unterausschuss Datenschutz ist darüber bis zum 31. Dezember 2010 zu berichten.

8. Kopien durch mitgebrachte Vervielfältigungsgeräte (16., Drs S. 151)

Der Senat wird aufgefordert, mit einem Rundschreiben an die öffentlichen Stellen Berlins darüber zu informieren, dass die Vervielfältigung von amtlichen Unterlagen durch vom Bürger mitgebrachte Geräte (wie Fotoapparat, Scanner) immer dann gestattet werden kann, wenn die materiell-rechtlichen Voraussetzungen für die Herausgabe von (ggf. geschwärzten) Kopien (z. B. nach § 13 Abs. 5 IFG) vorliegen.

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 17. Juni 2010 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2008

Frau Präsidentin,
sehr geehrte Damen und Herren,

ich möchte Ihnen zunächst für das einhellige Vertrauen danken, das Sie mir bei meiner erneuten Wahl zum Berliner Beauftragten für Datenschutz und Informationsfreiheit am 3. Juni 2010 ausgesprochen haben. Damit verbinde ich den Dank dafür, dass das Abgeordnetenhaus mit dem Haushaltsgesetz 2010/2011 entsprechend meinem Wunsch trotz der Haushaltsnotlage des Landes unsere Dienststelle personell verstärkt hat. Hierdurch hat das Parlament deutlich gemacht, dass es die wachsende Bedeutung von Datenschutz und Informationsfreiheit in der Bundeshauptstadt erkennt.

Wie dringend notwendig diese Verstärkung ist, macht auch der **Jahresbericht 2008** deutlich, der naturgemäß nur einen Teil unserer Tätigkeit beleuchtet und über den Sie heute beraten. Ich bin den Mitgliedern des Unterausschusses „Datenschutz und Informationsfreiheit“ sehr dankbar für die konstruktive Diskussion nicht nur dieses Berichts und der Stellungnahme des Senats, sondern auch anderer aktueller Fragen, die sich in den Bereichen des Datenschutzes und der Informationsfreiheit im vergangenen Jahr gestellt haben.

Der Unterausschuss hat die Ihnen vorliegende Beschlussempfehlung vorbereitet, die in sieben Punkten – eine Ziffer beruht auf einer redaktionellen Doppelung – den Senat zum Tätigwerden auffordert. Dabei ist bemerkenswert, dass der überwiegende Teil der Punkte erstmals den insofern verbesserungsbedürftigen Informationszugang der Bürger betrifft.

1. Das vorbildliche IT-Sicherheitsmanagement der Berliner Polizei soll in anderen Verwaltungen Schule machen.

2. Die Finanzverwaltung darf bei Vermietern nur die erforderlichen Daten der Mieter ermitteln.
3. Datenschutz muss endlich als Bildungsaufgabe in den Schulunterricht integriert werden.
4. Der Senat soll jährlich über den Einsatz von Lobbyisten in der Berliner Verwaltung berichten und die Einrichtung eines entsprechenden Registers prüfen.
5. Pauschale Geheimhaltungsabsprachen mit Vertragspartnern im Bereich der Grundversorgung sind künftig zu unterlassen. In diesem Punkt ist eine erfreuliche Ergänzung des Informationsfreiheitsgesetzes auf Initiative der Koalitionsfraktionen und der Fraktion Bündnis 90/Die Grünen in Vorbereitung, die ich im Grundsatz unterstütze, für die ich aber noch Verbesserungen vorgeschlagen habe.
6. Ein zentrales Internet-Portal für Verwaltungsvorschriften soll geschaffen werden, um die Transparenz in diesem Bereich zu erhöhen,

und

7. ein immer wieder auftretendes praktisches Problem soll dadurch gelöst werden, dass die öffentlichen Stellen Berlins den Bürgern im Rahmen der Bestimmungen die Benutzung von mitgebrachten Kameras oder Scannern gestatten, um Kopien von amtlichen Unterlagen zu machen.

Ein seit Jahren ungelöstes Datenschutzproblem betrifft die **Finanzierung der öffentlich-rechtlichen Rundfunkanstalten**. In der vergangenen Woche haben sich die Ministerpräsidenten der Länder auf ein neues Gebührenmodell verständigt, das künftig einen haushaltsbezogenen Rundfunkbeitrag vorsieht und Ermittlungen in der Privatsphäre von Rundfunkteilnehmern weitgehend überflüssig macht. Das ist zwar grundsätzlich zu begrüßen. Allerdings wirft auch das neue Modell noch zahlreiche datenschutzrechtliche Fragen auf, die bei der Formulierung des entsprechenden Staatsvertrags zu lösen sein werden. Ich würde es außerdem begrüßen, wenn die Länder bei diesem wichtigen Schritt nicht auf halber Strecke stehen blieben, sondern zugleich die **Gebühreneinzugszentrale**, eine der größten zentralen Datenbanken in Deutschland, **abschaffen** würden. Der ehemalige Bundesverfassungsrichter Paul Kirchhof hat das Vorgehen der GEZ als „inquisitorisch“ und rechtsstaatlich inakzeptabel bezeichnet. Der neue Rundfunkbeitrag kann durch andere Stellen, etwa die Finanzämter, erhoben werden.

Meine Damen und Herren,

Google Street View und Facebook sind nur zwei von vielen Schlagworten, die die wachsende Bedeutung des Datenschutzes in der heutigen Zeit belegen. Keine Datenschutzbehörde kann ausschließen, dass es künftig in Unternehmen und Verwaltung zu Problemen oder Rechtsverstößen kommt. Gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern verstehe ich es aber als meine Aufgabe, auf diese Probleme hinzuweisen und Lösungen zu entwickeln. Dabei hoffe ich weiterhin auf die Unterstützung dieses Hauses. Von Umberto Eco stammt der Satz: *„Das Problem ist nicht, die Privatsphäre zu schützen, sondern diejenigen zu erziehen, die ihr keinen Wert beimessen.“* Dieser Satz gilt in gleicher Weise für die Informationsfreiheit.

Herzlichen Dank für Ihre Aufmerksamkeit.

Stichwortverzeichnis

T

U

V

W

Z