Berliner Beauftragter
für Datenschutz und
Informationsfreiheit

DATEN
SCHUTZ

25 Jahre Datenschutz

5 Jahre Informationsfreiheit

in Berlin

Berlin

INFORMATIONS-
FREIHEIT

25 Jahre Datenschutz
5 Jahre Informationsfreiheit
in Berlin

Berlin · November 2004

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Informationsfreiheit

An der Urania 4 – 10, 10787 Berlin
Telefon: (0 30) + 1 38 89-0
Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: Druckerei Feller
überarbeiteter Nachdruck 2008

Inhaltsverzeichnis

Seite

Vorwort 5

Höhepunkte in 25 Jahren Dienst für Bürgerinnen und Bürger 7

Chronologie des Datenschutzes in Berlin 53

Ein Aufkleber und seine parlamentarische Behandlung 57

Zum Schluss: ein Silbenrätsel 59

Vorwort

Dr. Hans-Joachim Kerkau

Prof. Dr. Hansjürgen Garstka

Vor 25 Jahren, am 1. November 1979, nahm der erste Berliner Datenschutzbeauftragte Dr. Hans-Joachim Kerkau seine Amtsgeschäfte auf. Wie die anderen Datenschutzbeauftragten in Bund und Ländern trug er in den zehn Jahren seiner Amtszeit entscheidend dazu bei, aus den zunächst gleichermaßen unverstandenen und ungeliebten Grundsätzen des Datenschutzes wie Erforderlichkeit, Zweckbindung oder Auskunftsrechte nicht mehr wegzudenkende Garantien für die freie Entfaltung der Persönlichkeit auch unter den Bedingungen der Informationsgesellschaft zu entwickeln.

Bereits in dem Bericht zur Aufnahme seiner Tätigkeit noch im Jahr 1979 stellte er einen Zusammenhang zwischen dem Datenschutz und der Gewährung eines generellen Akteneinsichtsrechts her, mit der sich die öffentliche Verwaltung die für ein demokratisches Gemeinwesen angemessene Transparenz verschaffen sollte. Fast genau auf den Tag 20 Jahre nach der Eröffnung der Dienststelle wurde das Anliegen mit dem In-Kraft-Treten des Berliner Informationsfreiheitsgesetzes Wirklichkeit. Der Berliner Datenschutzbeauftragte war nunmehr Berliner Beauftragter für Datenschutz und Akteneinsicht; mit dem neuen Berliner Datenschutzgesetz wurde daraus im Juli 2002 der Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Zuvor hatte der Berliner Datenschutzbeauftragte bereits im Jahr 1995 die Aufgaben der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich übernommen. Kontrolle und Beratung der Privatwirtschaft konnten damit in der gleichen Weise gehandhabt werden wie zuvor gegenüber der öffentlichen Verwaltung.

Die vorliegende Broschüre stellt einige Höhepunkte unserer Tätigkeit in den vergangenen Jahren dar, natürlich ohne alle Aufgabenbereiche abdecken zu können. Die Auswahl soll aber zeigen, in welch vielfältiger Weise Datenschutz und Informationsfreiheit unsere Gesellschaft prägen.

Prof. Dr. Hansjürgen Garstka

Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Höhepunkte in 25 Jahren Dienst für Bürgerinnen und Bürger

1979

Es geht los

Das Gesetz über den Datenschutz in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) ist am 21. Juli 1978 verkündet worden und am Folgetag in Kraft getreten. Weit über ein Jahr hat es gedauert, bis nach personalpolitischen Meinungsverschiedenheiten der damaligen Koalitionsparteien SPD und FDP der parteilose Jurist und vormalige Direktor der Datenzentrale Baden-Württemberg, Dr. Hans-Joachim Kerkau, am 27. September 1979 vom Abgeordnetenhaus zum ersten Berliner Datenschutzbeauftragten gewählt wurde. Am Donnerstag, dem 1. November 1979, trat er sein Amt an. Im 12. Stock des damals immer noch imposant wirkenden Europacenters begann er, zusammen mit der ersten Chefsekretärin Monika Klössing die Plastikhüllen von den wenigen bereits von hilfreichen Verwaltungen beschafften Möbeln zu entfernen. Eine von der Kulturverwaltung im gleichen Haus zur Verfügung gestellte, dort bereits ausgemusterte elektromechanische Schreibmaschine war das erste informationstechnische Gerät in der Dienststelle.

Genau mit dieser Schreibmaschine wurde noch im gleichen Jahr der erste Tätigkeitsbericht, der „Bericht über die Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten“ gefertigt – in der damals allen vertrauten Papierklebetechnik. Die heute von jedem selbstverständlich genutzten Wordfunktionen „copy and paste“ waren damals mit samt aller heute zur Verfügung stehenden Computertechnik noch undenkbar.

Berichtet wird darüber, dass bis zum Jahresende bereits über 100 Eingaben eingegangen waren. Überrascht zeigte man sich über „Art und Umfang der Eingaben,

die die Personaldaten von Bediensteten der öffentlichen Verwaltung einschließlich ihrer Behandlung in Gerichtsverfahren“ betrafen. Insbesondere Beamte waren die ersten, die ihre Datenschutzrechte erkannten – jedenfalls wenn es um die eigenen Daten ging. Waren andere Bürgerinnen und Bürger betroffen, dauerte der Erkenntnisprozess länger. Wie man der folgenden Chronologie entnehmen kann, ist er auch nach 25 Jahren noch nicht abgeschlossen.

Ein überraschendes Thema wird im letzten Abschnitt dieses Berichts von 1979 angesprochen: „Schließlich wird der Datenschutz zunehmend im Zusammenhang mit der Frage zu sehen sein, ob sich die öffentliche Verwaltung nicht durch Gewährung eines generellen Akteneinsichtsrechtes die für ein demokratisches Gemeinwesen angemessene Transparenz verschaffen sollte“. Es sollte bis auf zwei Tage genau zwanzig Jahre seit der Eröffnung der Dienststelle dauern, bis dieses Anliegen Wirklichkeit wurde. Am 30. Oktober 1999 trat das Gesetz zur Förderung der Informationsfreiheit im Land Berlin (Berliner Informationsfreiheitsgesetz) in Kraft. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit erhielt die Aufgabe, das Recht auf Akteneinsicht und Informationszugang zu wahren.

1980

Zwei Menetekel

„MN MN TQL PRSN“ stand aramäisch kryptographiert an der Wand im babylonischen Kaiserpalast Belsazars nahe dem heutigen Bagdad, so berichtet die Bibel in Daniel 5,25. Daniel („Gott ist gerecht“), der herbeigeholte Sachverständige und spätere Reichskanzler unter Babylons Eroberer, dem Perserkaiser Kyros, interpretierte richtig: Gezählt, gezählt, gewogen, geteilt – die Ankündigung, dass das Reich untergehen wird.

Zwei Ereignisse im Jahr 1980 erscheinen als Menetekel für die Risiken, die viele Jahre später die Persönlichkeitsrechte und das inzwischen anerkannte Grundrecht auf informationelle Selbstbestimmung bedrohen werden. Die Informationstechnologie in Form von Computern und digitaler Telekommunikation tritt ihren Siegeszug auf dem Weg zur Informationsgesellschaft an. Fortan wird gezählt und gezählt, automatisch bewertet – und (aus-)geteilt.

In den intensiven Fahndungen nach dem „deutschem Herbst“ Ende der siebziger Jahre hatte das Bundeskriminalamt eine wie es schien geniale Idee: Da gesuchte RAF-Terroristen bei der Anmietung von konspirativen Wohnungen ein bestimmtes Verhaltens- und Eigenschaftsmuster zeigten (Barzahlung der Wohnungsmiete, geringer Stromverbrauch wegen ständiger Abwesenheit, Altersstruktur der Täter u. Ä.), könnte die entsprechende Analyse der Datenbestände von Wohnungsunternehmen, Energieversorgern, Meldeämtern und deren Zusammenführung vielleicht auf die Spur der Verdächtigen führen. Die Rasterfahndung war geboren. Sie führte ein einziges Mal in Frankfurt/Main zum Erfolg. Der Versuch der Wiederholung in Berlin im April 1980 führte zur Durchsuchung von 17.000 Wohnungen – ohne jedes Ergebnis.

Die Bewertung im Jahresbericht 1980 weist bereits auf das rechtsstaatliche Risiko hin, dem sich die Verteidiger des Rechtsstaats in den folgenden Jahrzehnten mehr und mehr gegenübersehen: „Die Frage, ob die durch Inanspruchnahme der elektronischen Datenverarbeitung entstandene Möglichkeit, größere Teile der Bevölkerung in die Fahndung einzubeziehen, eine neue Qualität polizeilichen Vorgehens darstellt, muss sorgsam erwogen werden. Die Gefahren dieser Methode könnten darin liegen, dass eine Rasterfahndung zu einer Umkehr der rechtsstaatlichen Beweislastprinzipien führt. An die Stelle der Unschuldsvermutung könnte auf Grund der Rasterfahndung die elektronisch erzeugte faktische Schuldvermutung treten“.

Bald war die Rasterfahndung gesetzlich geregelt. Als nach dem 11. September 2001 mit diesem Fahndungsinstrument nach terrorplanenden „Schläfern“ gefahndet wurde, wurden zwar bundesweit hunderttausende von Datensätzen abgeglichen, selbst vor Daten über die Religionszugehörigkeit wurde nicht Halt gemacht. Der Fahndungserfolg blieb aus: gezählt, gezählt, gewogen, aber – auch diesmal – ohne Resultat.

Im Juni 1980 startete in Berlin die Erprobung von Bildschirmtext. In einer Zeit, in der das Internet noch ein Gegenstand militärischer und allenfalls wissenschaftlicher Forschung war, bot die damalige Bundespost ihren Kunden einen Dienst an, mit dem sie Daten, die Anbieter verschiedenster Lebensbereiche zwar nicht im „Netz“, wohl aber auf den Rechnern der Bundespost abgelegt hatten, mithilfe umständlicher Technik unter Verwendung des Telefons auf den heimischen Fernsehapparat herunterladen konnten.

Der Berliner Datenschutzbeauftragte wurde in die dafür erforderliche Gesetzgebung einbezogen – die Geburtsstunde nicht nur des Arbeitskreises Medien der Konferenz der deutschen Datenschutzbeauftragten, sondern im Gefolge auch der

International Working Group on Data Protection in Telecommunications, die als „Berlin Group“ inzwischen hohes internationales Ansehen genießt. Die heutige Struktur der datenschutzrechtlichen Spezialregelungen im deutschen und auch internationalen Telekommunikationsrecht geht auf die Diskussionen in diesen Gremien zurück.

Schon damals wurden die Risiken erkannt, die uns heute bei der Bewertung des Internet verfolgen. Aus den Daten, die beim Betrieb dieser Systeme entstehen, könnten „Teilnehmerprofile über Art und Umfang der Benutzung erstellt werden. Mit anderen Informationssystemen zusammengeführt, können sie wesentlich zur Erstellung verfassungsrechtlich nicht zulässiger Persönlichkeitsprofile beitragen. Darüber hinaus können Schlüsse auf weitergehende Verhaltensweisen gezogen werden … die auch den verfassungsrechtlich absolut geschützten Intimbereich betreffen können“. Gezählt, gezählt, gewogen …

1981

Das Datenscheckheft

Im Herbst 1981 erschien die erste Fassung des Datenscheckheftes. Damit wurde eine alte Idee von Hans-Joachim Kerkau Wirklichkeit, dem Bürger Hilfsmittel in die Hand zu geben, mit denen er seine im Datenschutzgesetz verbrieften Rechte korrekt und effektiv wahrnehmen konnte, insbesondere sein Recht auf Auskunft bei öffentlichen Stellen. Der Einband war den damals gebräuchlichen Euroschecks nachgebildet, innen fanden sich vorgedruckte Postkarten und Hinweise zu ihrer Nutzung. Da die Presse dem Erscheinen des Datenscheckheftes lebhaftes und freundliches Interesse schenkte, war die Erstauflage von 6.500 Exemplaren im Nu vergriffen. Die gleich starke zweite Auflage war ebenfalls zum Erscheinen des Jahresberichts 1981 vergriffen.

Natürlich wurde das Datenscheckheft von den Bürgern auch intensiv genutzt. Waren vorher datenschutzrechtliche Auskunftsersuchen eher selten, weil eine aktive Unterrichtung der Bürger über ihre Datenschutzrechte noch nicht erfolgt war, so stieg jetzt die Anzahl von Anträgen gewaltig an. Hauptsächlich betroffen war die Polizei, die damals noch die Verantwortung über das Melde-, KfZ- und

Führerscheinwesen und somit durchaus komplexe Anfragen zu bewältigen hatte. Der damalige Innensenator Lummer reagierte empört und warf dem Berliner Datenschutzbeauftragten vor, er wolle mit dem Datenscheckheft die Funktionsfähigkeit der Polizei beeinträchtigen. Die Polizei passte sich jedoch an, indem sie effiziente Arbeitsverfahren zur Bearbeitung der Bürgeranfragen einführte, letzten Endes ein gewünschter Nebeneffekt des Datenscheckheftes.

In der Folge hat das Datenscheckheft in Inhalt und Form zahlreiche Aktualisierungen und Verbesserungen erfahren. Inzwischen liegt das Datenscheckbuch online vor, so dass die Musterschreiben über das Internetprogramm www.datenschutz-berlin.de abgerufen werden können.

Wahlrechtsentzug durch Nummerndreher

Ein Bürger erhielt zur Abgeordnetenhauswahl im Mai 1981 keine Wahlunterlegen. Es stellte sich heraus, dass fünf Jahre zuvor in seinen Datensatz eine Pflegschaft eingetragen worden war, was automatisch zum Entzug der Wahlberechtigung führte. Das zum Nachweis der Pflegschaft eingetragene Aktenzeichen des Amtsgerichtsbeschlusses betraf allerdings eine ganz andere Person. Die zwölfstelligen Ordnungsmerkmale der beiden Betroffenen wiesen starke Ähnlichkeiten auf. Offensichtlich war bei der Abfrage ein falsches Ordnungsmerkmal eingegeben worden, was auch mit der Prüfziffer nicht erkannt werden konnte. Ein solcher Fehler kann nicht mehr wiedergefunden werden, solange er sich nicht – wie in diesem Falle – bemerkbar macht.

Eine spätere Umfrage ergab, dass in Berlin (West) mindestens in 50 Fällen Bürger wegen fälschlich eingetragener Pflegschaften keine Wahlunterlagen erhalten hatten. Da zahlreiche Fälle dieser Art ohne formelle Einsprüche bereinigt worden waren, war von einer hohen Dunkelziffer auszugehen.

Die Gründe für diese Fehleintragungen waren verschiedener Art, der oben beschriebene Grund war sicher ein exotischer Einzelfall. Erst unser Eingreifen führte dazu, dass die Eintragung von Pflegschaft in die Einwohnerdatenbank vom Amtsgericht gegengeprüft werden und dass das Ordnungsmerkmal der Meldebehörde nicht allein für den Zugriff auf Meldedaten ausreichen darf.

Schon damals haben wir gefordert, dass sich vergleichbare Kontrollen auch auf andere sensible Daten der Einwohnerdatenbank erstreckten sollten. Aber erst als

Jahre später mehrere Vorfälle mit falsch eingetragenen Haftunterbringungen bekannt wurden, wurde im Berliner Meldewesen eine Revision der Eintragung sensibler Daten eingeführt.

1982

Ganz was Neues: Die Dezentralisierung der Datenverarbeitung

Der Fortschritt der Informationstechnik hat die datenschutzrechtlichen Entwicklungen schon früh geprägt. Etwa um 1982 gewann der dezentrale Zugriff auf Datenbestände auch in der Berliner Verwaltung praktische Relevanz. Wurde die Datenverarbeitung zuvor in abgeschlossenen Rechenzentren betrieben, die ihre Aufträge abarbeiteten und Berge von Computerausdrucken mit Fahrdiensten verteilten, so bekamen vereinzelte Arbeitsplätze in der Verwaltung jetzt direkten Kontakt zum Computer. Aus einer Ansammlung singulärer Rechenzentren entstand allmählich eine informationstechnische Infrastruktur, in der Daten über größere Entfernungen übertragen werden konnten. Nachrichten- und Datenübertragungstechnik wurde mit Verarbeitungstechnik kombiniert. Staunend wurde konstatiert, dass die „Neuen Medien“, damals in Form der ersten Bildschirmtextgeneration, dazu führten, dass der Informationszugang vor Organisationsgrenzen nicht mehr Halt machte, sondern sogar jedermann an solchen Diensten teilhaben konnte.

Diese technische Entwicklung bedeutete auch, dass der Datenschutzbeauftragte sich auf neue Anforderungen bei der rechtlichen Bewertung von Datenflüssen und bei der Umsetzung wirksamer technischer und organisatorischer Maßnahmen einzustellen hatte. Die Kontrolle klassischer Rechenzentren begann an Bedeutung zu verlieren. Bedeutsamer wurde der Schutz der Daten auf den Übertragungswegen und an den an Netze angeschlossenen Arbeitsplätzen in der Verwaltung. Dies war schon deshalb bedeutsam, weil „normale“ Verwaltungsmitarbeiter, die jetzt mit den Segnungen moderner Informationstechnik konfrontiert wurden, anders als die Datenverarbeitungsprofis in den Rechenzentren an den sicheren Umgang mit der Datenverarbeitung und den von ihr erzeugten Arbeitsergebnissen mit personen-

bezogenen Daten noch nicht gewöhnt waren. Nicht die professionelle Datenverarbeitung barg die Risiken für die sichere Verarbeitung, sondern die Nutzung ihrer Daten durch die Anwender.

Was war noch bemerkenswert in technischer Hinsicht? Die ersten Personalcomputer kamen auf und stellten den datenschutzgerechten Umgang mit personenbezogenen Daten vor neue Herausforderungen. Erste Auslagerungen von Datenverarbeitungsaufgaben auf private Unternehmen kamen vor. Outsourcing begann, ohne dass es dieses Wort schon gab. Eine Entwicklung zeichnete sich ab, die uns auch heute noch intensiv beschäftigt.

Im Fokus: Das Bauwesen

Das Bau- und Planungswesen geriet 1982 aus verschiedenen Anlässen ins Visier des Datenschutzbeauftragten. Meistens ging es um die Frage, wer wann wie bei welcher Gelegenheit über bau- oder mietrechtliche Vorgänge zu informieren war. In der Berliner Verwaltung, speziell in den Bezirken, gab es große Verunsicherung mit der Folge sehr unterschiedlicher Vorgehensweisen:

Durften die Mietpreisstellen der Bezirke im Rahmen von Mietpreiserhöhungen im damals mietpreisgebundenen Wohnungsbau vollständige Datensätze über Mieter und deren Angehörige an alle anderen Mieter des betroffenen Hauses versenden? Natürlich nicht, und so wurde dies beanstandet.

Durften Bezirksämter Mietern mitteilen, dass der Eigentümer eine Abgeschlossenheitsbescheinigung beantragt hatte und daher möglicherweise eine Umwandlung in Eigentumswohnungen bevorstand? Nicht ohne Einwilligung, solange der Status einer wirtschaftlichen Planung des Eigentümers nicht überschritten war.

Durfte sich die Senatsverwaltung für Bau- und Wohnungswesen beliebig der Daten des elektronischen Liegenschaftskatasters der Bezirke bedienen? Nein, nur im konkreten Einzelfall!

Weitere einschlägige Themen in jenem Jahr: Veröffentlichung personenbezogener Daten im Bebauungsplan, Behandlung von Mieterdaten bei Sanierungsvorhaben, Datenerhebung für die Fehlbelegungsabgabe. Die ebenfalls schon diskutierte Frage, wer unter welchen Umständen Einsicht in die Bauakten erhalten sollte, wird erstaunlicherweise vielleicht noch im Jahr 2004 gesetzlich geregelt.

1983

Volkszählungsurteil: Das Jahr der Herausforderung

Und dabei fing alles so ruhig an.

Im März 1982 hatte der Bundestag, ohne dass es zu wesentlichen Diskussionen kam, das Gesetz zur Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung für das Jahr 1983 beschlossen. Anfang 1983 informierte die Amtliche Statistik über die bundesweite Aktion. Für Berlin wurden 20.000 Interviewer geworben.

Aber die Zählung hatte nicht nur Freunde. Im Januar 1983 formierte sich in Berlin wie auch im Bundesgebiet ein von Tag zu Tag wachsender Widerstand gegen die Zählung. Die Diskussion war von Schlagzeilen geprägt wie „Großer Bruder lässt zählen“, „Politiker fragen – Bürger antworten nicht“, „Nein zum Schäfchenzählen“. Nach und nach wurde allen bewusst, dass Datenschutz nichts Abstraktes ist, das in Elfenbeintürmen ersonnen wurde, sondern jeden Einwohner berührt. Die Volkszählungsgegner nahmen sich die gescheiterte holländische Volkszählung von 1971 zum Vorbild. Dort hatten 30 % der Niederländer falsche oder gar keine Angaben gemacht. So gab es in einem kleinen Dorf laut Statistik etliche Eheleute unter 15 Jahren. Aber auch Berufe wie „Heiratsschwindler“ u. ä. waren keine Seltenheit. Meldungen wie „Kopfprämie für Volkszähler“, „München zahlt für das Aufspüren nicht gemeldeter Personen“ sorgten nicht gerade für eine Beruhigung der Situation. Für Verwirrung sorgten Äußerungen von Franz Josef Strauß, dass die Volkszählung völlig unsinnig sei. Das Schlagwort vom „Volksverhör“ ging um. Mitte März 1983 stoppte als erstes Bundesland Hamburg die Vorarbeiten für die Zählung. Nach und nach wurden von den Volkszählungsgegnern Verfassungsbeschwerden beim Bundesverfassungsgericht eingereicht, am Ende waren es mehr als Tausend.

Endlich – Ende März 1983 – nahm die Konferenz der Datenschutzbeauftragten von Bund und Ländern Stellung und verwies auf eine Reihe von Unklarheiten und Schwachstellen im Volkszählungsgesetz. Hans-Joachim Kerkau stellte dem Innensenator 20 Forderungen. In ihrer Not sagte die Innenverwaltung am 28. März 1983 die Erfüllung aller Forderungen zu.

Gleichzeitig heizten aber die ersten Bußgeldbescheide über 3.000 DM wegen des Boykottaufrufs das Klima weiter an. Ostern kam es zur ersten öffentlichen Verbrennung von Fragebögen vor der Gedächtniskirche. Die Innenverwaltung drohte

denjenigen, die ihre Fragebögen vernichten, mit Strafanzeige wegen Sachbeschädigung. Gegen die taz wurden strafrechtliche Ermittlungen eingeleitet.

Am 12. April 1983 begannen in Berlin die Schulungen für die 20.000 Zähler. Am nächsten Tag sollte das Bundesverfassungsgericht über den Antrag auf eine einstweilige Anordnung, die Volkszählung auszusetzen, entscheiden. Zeitungen sprachen von einem „Verfassungstoto". Das nicht mehr existierende Berliner Volksblatt kommentierte: „Als Diplomat und ‚Brückenschläger' zwischen volkszählendem Staat und besorgtem Bürger zeigte sich gestern der oberste Datenschützer Berlins. Wie er bei einer Pressekonferenz durchblicken ließ, rechnet er damit, dass das Bundesverfassungsgericht heute das geplante Verfahren bei der Zählung korrigieren wird im Interesse ihrer Kritiker… . Angesichts der ‚biegsamen' Haltung des Berliner Datenschutzbeauftragten in Sachen Volkszählung wird sich wohl (der damalige Innensenator) Heinrich Lummer als der Stärkere erweisen."

Und dann kam der „Supergau" für die Statistik. Die Volkszählung war auszusetzen bis zur endgültigen Entscheidung. BILD schreibt: „Keine Volkszählung! 200 Millionen verpulvert". Lummer: „Ich stifte der Kirche eine Kerze. Sie möge das Verfassungsgericht erleuchten."

Nun begannen nicht nur für die Verfassungsrichter, sondern auch für Datenschützer wie Statistiker, Innenminister und Regierungen von Bund und Ländern die „Mühen der Ebene" mit dem Erstellen von Gutachten, Stellungnahmen, dem Erarbeiten von Rechtspositionen. Die Verfassungsrichter in Karlsruhe hatten sich mal wieder als „Spielverderber" (taz, 14. April 1983) erwiesen.

Am 15. Dezember 1983 wurde das Urteil verkündet. Das Volkszählungsgesetz war teilweise verfassungswidrig, die Volkszählung durfte nicht durchgeführt werden. Die Richter nahmen den Fall zum Anlass, aus den Artikeln 1 und 2 des Grundgesetzes ein neues Grundrecht abzuleiten: das Grundrecht auf informationelle Selbstbestimmung. In Anlehnung an einen Satz, den bereits 1890 in dem bahnbrechenden Aufsatz „The Right to Privacy" der damalige Bostoner Anwalt und spätere Oberste Bundesrichter Louis Brandeis formuliert hatte, stellten sie dem Urteil den Leitsatz voran:

„Das Grundrecht gewährleistet … die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Das Urteil sollte zur Grundlage bahnbrechender Neuerungen im Datenschutzrecht werden; in vielen weiteren Entscheidungen des Bundesverfassungsgerichts

und anderer Gerichte aller Instanzen wird es später zum wichtigsten Angelpunkt für die juristische Bewältigung der Informationsgesellschaft werden.

Übrigens, beinahe hätte es eine Schlägerei im Bundesverfassungsgericht gegeben. Der Vertreter der Bundesregierung Badura geriet massiv mit dem Präsidenten des Bundesverfassungsgerichts Ernst Benda aneinander. Badura knöpfte sich die Jacke auf, trat ans Rednerpult und sagte zu Benda, er sei jetzt „zu einer Art Wortgefecht“ bereit. Er fing sich erst wieder nach eingehender Belehrung durch den Präsidenten.

1984

Computerkriminalität: Hacking, Phishing, Sabotage …

Man mag nachträglich darüber diskutieren, wieweit Orwells bereits 1948 für „1984“ erdachte Vision vom „Großen Bruder“ vor 20 Jahren schon eine reale Bedrohung war. Dass sie heute nach wie vor ernstzunehmen ist, beweisen „Großer Lauschangriff“, allgegenwärtige Videoüberwachung oder die Forderung der Sicherheitsbehörden, alle Nutzungsdaten im Internet jahrelang aufzubewahren.

Tatsächlich stand 1984 die wachsende Furcht vor der Manipulierbarkeit der Datenverarbeitungssysteme durch Computerkriminalität im Brennpunkt der Arbeit des Datenschutzbeauftragten. Bereits ohne Internet machten sich Unbefugte einen Sport daraus, Datenverarbeitungssysteme, die über Telefon-, Kabel oder DATEX-Netze erreichbar waren, anzuwählen, die meist schwachen Schutzvorkehrungen zu überwinden und die Systeme für eigene Zwecke zu nutzen (Zeitdiebstahl), in Verarbeitungsprozesse einzugreifen oder gar Zugriff auf schutzwürdige Daten zu erlangen. Sogenannte Hacker erhielten ungeahnte Publizität, sonnten sich in der Sympathie der Leute, denen die „Macht der Computer“ sowieso ein Dorn im Auge war, und fühlten sich als moderne „Robin Hoods“.

Die Hacker wählten die Rufnummern von DV-Systemen an, die in der Regel nicht streng geheim gehalten wurden, und mussten dann die Kontrollmaßnahmen überwinden, die meist in der Eingabe eines geheimen Passworts bestanden. Alsdann wurde versucht, durch das Ausprobieren von Passwörtern das Richtige zu finden. Fündig wurde man häufig mit Begriffen aus dem Lebensbereich berechtigter Benutzer wie Namen, Nachnamen, Geburtstag der Freundin, Automarke

oder -kennzeichen. Erfolgversprechender war noch das sog. „Social Engeneering“. Unter diesen Begriff fiel das Übertölpeln von Berechtigten oder gar von Systemverwaltern, so dass diese die geheimen Codes offenbarten, eine Frühform des heute aktuellen „Phishing“ (password fishing). Auch das rechnergestützte Ausprobieren von Passwörtern war schon Praxis, wenn auch angesichts der damaligen Rechnerkapazitäten noch harmloser als heute.

Erfahrungen aus den USA, die schon stärker mit Computern durchsetzt waren und in denen das Hacking ebenfalls fortgeschrittener war, zeigten, dass die Verbreitung von PCs in Privathaushalten, der Vernetzungsgrad von DV-Systemen, die Vielfalt der verschiedenen Wählnetze und deren geringer Sicherheitsstandard, der geringe Sicherheitsstandard der angeschlossenen Systeme und der geringere Stellenwert der Ordnungsmäßigkeit der Datenverarbeitung in den USA das Hacking begünstigten. In Deutschland gab es dagegen einheitliche Wählnetze mit recht hohem Sicherheitsstandard, bedingt durch das Postmonopol, sowie ohnehin höhere Sicherheitsstandards wegen der bestehenden gesetzlichen Anforderungen.

Als Maßnahmen gegen das Hacking wurde die Isolierung der Rechner vorgeschlagen, ansonsten die Einrichtung geschlossener Nutzergruppen in den Wählnetzen, automatische Rückrufkontrollen sowie besondere Sorgfalt bei den sonstigen Sicherheitsmaßnahmen, insbesondere hinsichtlich der Geheimhaltung von Passwörtern. Diese Maßnahmen hatten in den Folgejahren das Hacking zurückgedrängt. Dies änderte sich mit dem Aufkommen des Internet schlagartig, mit dem nach und nach fast alle Computer der Welt vernetzt werden. Hacking zum Zwecke der Erlangung wichtiger Geheimnisse ist heute eine der wichtigsten Formen der Computerkriminalität.

Das sah man 1984 noch anders. Hacking wurde gegenüber anderen Formen der Computerkriminalität abgegrenzt, indem Hackern eher sportlicher Ehrgeiz als kriminelle Energie unterstellt wurde. Zur eigentlichen Computerkriminalität wurden gezählt: Sabotage, vorsätzliche Sachbeschädigung, Diebstahl gefüllter Datenträger, Daten- und Programmmanipulationen, unbefugter Abruf und Kopieren von Daten, Offenbarung geschützter Daten, Anzapfen von Datenleitungen.

Wissenschaftliche Untersuchungen hatten bereits damals festgestellt, dass 95 % der Fälle von Computerkriminalität von Mitarbeitern der datenverarbeitenden Stellen selbst begangen oder unterstützt werden. Bei den übrigen 5 % lag fast immer die Vernachlässigung der technischen und organisatorischen Kontrollmaßnahmen vor. Die Manipulation von Daten zum Zwecke der persönlichen Bereicherung war aus dem öffentlichen Bereich Berlins seinerzeit noch nicht bekannt geworden. Dies wurde in späteren Jahren dann aber nachgeholt.

1985

PCs – die kleinen, großen Brüder

Ende der 70er Jahre begann die Revolution in der Datenverarbeitung, ohne die die heutige Verbreitung der automatisierten Datenverarbeitung undenkbar gewesen wäre: Die ersten Personal Computer (PC) wurden auf den Markt gebracht, meist von Unternehmen, die es heute gar nicht mehr gibt.

Mitte der 80er Jahre drangen diese PCs auch in die Berliner Verwaltung vor. Kleine Anwendungsbereiche, für die sich der Einsatz von Großrechnern nicht lohnte, konnten nun mit automatisierter Datenverarbeitung unterstützt werden. Da die Vernetzung solcher Rechner noch in den Kinderschuhen steckte, gab es zunächst fast nur Stand-Alone-Lösungen, manchmal teilten sich mehrere Mitarbeiter einen Rechner. Es gab zwei verschiedene Modelle von PC-Anwendungen: Zum einen gab es „Konfektionssysteme“, Rechner, die samt Anwendungssoftware mehr oder weniger „schlüsselfertig“ ausgeliefert wurden, so dass für die Nutzung keine oder nur einfache Anpassungen erforderlich wurden. Zum anderen wurden PCs auf Veranlassung einzelner Mitarbeiter beschafft oder gar von ihnen privat zur Verfügung gestellt. Die Anwendungsprogramme wurden von diesen Autodidakten erstellt und in der Regel auch selbst genutzt.

Der Einsatz privater Computer zu dienstlichen Zwecken wurde aus guten Gründen von der Senatsverwaltung für Inneres streng reglementiert, um den ordnungsgemäßen Arbeitsablauf der Verwaltung für alle Streitfälle zu wappnen. Im Ergebnis bedeuteten die Regelungen, dass der Einsatz von privaten Rechnern zu dienstlichen Zwecken kaum genehmigungsfähig war. Gleichwohl war die Entwicklung nicht zu stoppen. Insbesondere Bedienstete, die regelmäßig zu Hause arbeiten wie Lehrer oder Richter, waren von dienstlicher Nutzung privater PCs nicht abzuhalten. Für die genannten Personengruppen wurden deshalb eigene gesetzliche Regelungen geschaffen – es kann bezweifelt werden, dass sich alle Beteiligten daran hielten.

Der Berliner Datenschutzbeauftragte gab eine Broschüre mit „PC-Grundsätzen“ heraus, die der übergreifenden Forderung praktische Umsetzbarkeit verleihen sollten, dass personenbezogene Daten nicht deshalb schlechter geschützt sein dürfen, weil sie auf einem PC verarbeitet werden. Dies war damals keine Selbstverständlichkeit, weil der Glaube verbreitet war, dass dann, wenn die Com-

puter schon kaum noch etwas kosten, auch für die technisch-organisatorische Sicherheit der Verarbeitung selbst sensibler Daten nichts oder wenig ausgegeben werden müsste.

1986

Das Melderecht: Vom Schrittmacher zum Schlusslicht

Mit dem Melderechtsrahmengesetz von 1980 waren erstmalig grundlegende datenschutzrechtliche Regelungen für die Erfassung der Einwohner geschaffen worden. Die Länder hätten die Vorgaben innerhalb von zwei Jahren umsetzen müssen, was in Berlin nicht gelungen war. Wegen zahlreicher Meinungsverschiedenheiten hatte man ein Gutachten des nunmehr im Ruhestand weilenden Ernst Benda eingeholt. Besonders strittig war, ob der Polizeipräsident in Berlin weiterhin für Ordnungsaufgaben zuständig sein sollte. Zwar waren mehr als hundert Jahre seit einem Urteil des Preußischen Oberverwaltungsgerichts vom 14. Juni 1882 vergangen, wonach es nicht nur nicht Aufgabe der Polizei ist, die Sichtachse zwischen Kreuzbergdenkmal und Stadtschloss freizuhalten, sondern diese sich überhaupt auf Strafverfolgung und Gefahrenabwehr zu beschränken habe. Die Berliner Polizei war aber sogar im Jahr 1995 neben dem Meldewesen auch noch für andere Ordnungsaufgaben wie das Ausländer- und Kraftfahrzeugwesen zuständig. Benda machte sich für die „Entpolizeilichung“ des Meldewesens stark. Benda überzeugte. Am 1. April 1986 war es dann so weit: Das neu gegründete Landeseinwohneramt nahm seine Arbeit auf.

Auch in anderer Hinsicht hatten sich die Diskussionen gelohnt. Berlin bekam eines der fortschrittlichsten Meldegesetze in der Bundesrepublik. Ein automatisiertes Abrufverfahren auf bestimmte, abschließend festgelegte Felder der Datensätze der Einwohner stellte sicher, dass die Polizei jederzeit auf die für sie erforderlichen Daten auch außerhalb der Dienstzeiten des Landeseinwohneramtes zugreifen konnte. Eine Gefährdung der öffentlichen Sicherheit, die die Polizei lautstark befürchtet hatte, ist zu keiner Zeit eingetreten.

Allerdings ist Berlin im Meldewesen mittlerweile das Schlusslicht in der Republik. Die Änderungen des Melderechtsrahmengesetzes von 1994 sind bisher ebenso wenig wie die der Jahre 2000, 2002 und 2003 in das Landesrecht übernommen worden. Auch viele von uns seit Jahren vorgelegte Empfehlungen zur Fortentwicklung des Melderechts in Berlin sind bisher nicht umgesetzt worden.

1987

Keine Volkszählung ohne Pannen

Das Volkszählungsurteil hatte auch die Grundlagen der Amtlichen Statistik in Frage gestellt. Deshalb wurde 1985 zunächst das Bundesstatistikgesetz novelliert und parallel dazu das Gesetz für eine neue Volkszählung im Mai 1987 verabschiedet. Die Datenschutzbeauftragten waren gefordert, auf das exakteste Einhalten der gesetzlichen Vorschriften zu achten. Da dies auch im Interesse der Statistiker lag, war die Kooperation sehr eng.

Es gab eine ganze Reihe von Problemen, die zu klären waren. So war unklar, ob die alliierten Behörden ein Zugriffsrecht auf die Einzeldaten der Volkszählung haben. Auf Unverständnis stieß, dass für die Gebäudevorerhebung Merkmale der Grundsteuerstellen schon eingetragen waren. Auch die Frage nach Namen und Anschrift der Arbeitsstätte, Schule oder Hochschule weckte Misstrauen. Besonders aufmerksam verfolgten wir den Umgang mit den Daten derjenigen Personen, die die Auskunft verweigert hatten und gegen die ein Bußgeld verhängt werden sollte. Noch Jahre später fanden wir bei einer Prüfung im Statistischen Landesamt „vergessene“ Dateien mit Verweigerern, obwohl es hierzu bereits lange eine faktische Amnestie gegeben hatte. In diesen Dateien waren teilweise sogar ganze „Verweigerer-Familien“ gespeichert.

Bei der Durchführung der Zählung gab es „Pleiten, Pech und Pannen“. Mal wurden einem Bürger Auskünfte dreimal abverlangt und er antwortete damit auch

dreimal. Dann wieder hatten die Interviewer keine Umschläge zur postalischen Rücksendung der Volkszählungsunterlagen für Selbstausfüller dabei. Auch wurden versehentlich Erhebungsunterlagen, die bereits von anderen Auskunftspflichtigen ausgefüllt worden waren, erneut, diesmal aber an andere Bürger versandt. Sinnloserweise war es zunächst den Erhebungsstellen verboten, ohne Rückfrage bei den Auskunftspflichtigen logisch zwingende Ergänzungen selbst vorzunehmen, beispielsweise zum Familienstand eines zweijährigen Kindes. Bei den Verweigerern war es nicht selten, dass sie den Anhörungsbogen mehrfach zugesandt bekamen, ebenso auch den Bußgeldbescheid. Dazu gehörten auch Bürger, deren Volkszählungsbriefe und Bögen nachweislich in den Ämtern versehentlich ungeöffnet vernichtet worden waren.

Auf der anderen Seite wandelte sich der Widerstand gegen die Volkszählung. So wurden zwar häufig die Bögen abgegeben, jedoch schlecht oder zum Teil falsch ausgefüllt. So fanden sich merkwürdige Berufe auf den Bögen wie „Lebenskünstler“ oder „Schlangenbeschwörer“. Als Arbeitgeber eines Pfarrers tauchte „Vater und Sohn“ auf; aber auch ein Kater Carlo wurde als Haushaltsmitglied gemeldet. Als genutztes Verkehrsmittel wurde den Statistikern etwas von einer Rikscha mitgeteilt. Das wesentlichste Mittel der Zählungsgegner war der verzögerte Rücklauf. BILD berichtete allerdings auch, dass einige Zähler, die zu faul zum Treppensteigen waren, zum Verdruss beitrugen, da den Betroffenen statt eines Erhebungsbogens als erstes ein Bußgeld angedroht wurde.

Ingesamt hatten 1987 etwa 225.000 Berliner die Volkszählung boykottiert. Nicht nur eine Berliner Spezialität war, dass Volkszählungsboykotteure, die die Heftnummern von den Erhebungsbögen abgeschnitten hatten, wegen Sachbeschädigung in das bundesweite Informationssystem der Polizei APIS eingespeichert wurden. Wir überprüften diese Datei für Schwerstkriminalität und Terrorismus. 68 der 75 Speicherungen in APIS wurden beanstandet.

Zur Hochform lief die Finanzverwaltung auf, als es darum ging, die verhängten Erzwingungs- und Bußgelder zu vollstrecken. Finanzsenator Rexrodt ordnete an, aus den Steuerakten von 6.000 Volkszählungsverweigerern Bankverbindungen und Kontonummern zu entnehmen. Ein Vollstreckungsbeamter beobachtete, wie ein Auskunftspflichtiger aus seinem Pkw ausstieg, notierte das Kennzeichen und machte eine Halterabfrage. Dabei wurde dessen Bankverbindung ausgedruckt. Die Informationen wurden dazu genutzt, die Bankkonten zu pfänden. Polizei und Vollstreckungsbeamte der Oberfinanzdirektion verschafften sich mit Bohrer und Säge Zugang zur Wohnung einer alten Dame, die von der Volkszählung weder etwas gehört hatte noch auf die Schreiben reagierte. Der Beamte pfändete die Handtasche der 88-Jährigen.

1988

4 Jahre nach 1984: Die Videoüberwachung wird zum Thema

Anlass war der Einsatz eines Fahndungsfotos, das mit einer Videokamera am Geldautomaten einer Bank aufgenommen wurde, als der Täter eine seinem Opfer entwendete ec-Karte missbräuchlich zum Bargeldabheben eingesetzt hatte.

Es gab noch keine spezielle datenschutzrechtliche Regelung für die Videoüberwachung, so dass wir uns bei der Beurteilung der Rechtmäßigkeit auf ein Gesetz berufen mussten, dessen Kernaussagen zum „Recht am eigenen Bilde“ seit dem Jahre 1907 im „Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie“, landläufig auch als Kunsturhebergesetz bekannt, festgeschrieben sind. Nach § 24 dieses Gesetzes ist es Behörden im öffentlichen Interesse erlaubt, ausnahmsweise für Zwecke der Rechtspflege und der öffentlichen Sicherheit Bildnisse ohne Einwilligung der Berechtigten sowie des Abgebildeten oder seiner Angehörigen zu vervielfältigen, zu verbreiten und öffentlich zur Schau zu stellen. Die Nutzung des Fotos zur Fahndung konnte mithin datenschutzrechtlich nicht beanstandet werden.

Gleichwohl mussten wir uns überlegen, wie man mit der Beobachtung von Personen durch Videokameras und erst recht mit der Aufzeichnung der Aufnahmen datenschutzgerecht umgehen kann. Es gab Stimmen, die meinten, dass es sich hierbei nicht um Probleme des Datenschutzes handelte. Für uns war klar, dass es sich bei den Aufnahmen um personenbezogene Daten, also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Absatz 1 Bundesdatenschutzgesetz) handelte. Wir mahnten klare gesetzliche Regelungen sowohl für den öffentlichen als auch für den privaten Bereich an.

Bis zur Realisierung dieser Forderung sind noch 13 Jahre ins Land gegangen. Erst das Bundesdatenschutzgesetz 2001, das die Europäische Datenschutzrichtlinie umsetzte, griff das Problem im Hinblick auf die Anmerkung im Erwägungsgrund 14 der Richtlinie auf, „personenbezogene Bild- und Tondaten“ in den Anwendungsbereich des Gesetzes einzubeziehen (allerdings nur die Beobachtung, nicht das Belauschen).

In unserem Jahresbericht 1988 finden sich wesentliche Anregungen, die letztlich ihren Niederschlag in § 9 b des BDSG bzw. 31 b BlnDSG gefunden haben:

- Differenzierung zwischen der reinen Beobachtung mit Videokameras und Monitoren und der Aufzeichnung (Speicherung) der Bilddaten, was einen ungleich tieferen Eingriff in die Persönlichkeitsrechte der Betroffenen darstellt,
- Abwägung nach dem Prinzip der Verhältnismäßigkeit zwischen dem Eingriff in die Persönlichkeitsrechte der Betroffenen und den Interessen der „Überwacher“,
- unverzügliche Löschung von aufgezeichneten Bilddaten, sobald sie für die Zweckerfüllung nicht mehr benötigt werden,
- Pflicht zum Hinweis auf die Videoüberwachung.

1989

11. Internationale Konferenz der Datenschutzbeauftragten in Berlin

Der Bundesdatenschutzbeauftragte Alfred Einwag hatte die Internationale Konferenz der Datenschutzbeauftragten, die seit einer Initiative des hessischen Datenschutzbeauftragten Spiros Simitis im Jahr 1978 jährlich zusammenkommt, für August 1989 nach Berlin eingeladen. Sie tagte unter unserer Mithilfe im Reichstagsgebäude, an dessen Rückwand gerade noch die Mauer entlanglief. Die Konferenz bereicherte auch die gleichzeitig stattfindende Internationale Funkausstellung mit einem Symposium zu Datenschutzfragen. Einer der Redner war der australische Datenschutzbeauftragte Kevin O’Connor.

In der Geschichte der Internationalen Datenschutzkonferenz ist diese 11. Sitzung in mehrfacher Hinsicht bedeutsam:

Erstmals hielt mit Pal Könyves-Toth, einem Mitarbeiter des Budapester John-von-Neumann-Instituts und des späteren ungarischen Datenschutzbeauftragten, ein Vertreter der – noch – sozialistischen Staaten Osteuropas eine flammende Rede zum Grundrecht auf informationelle Selbstbestimmung.

Peter Hustinx, damals Datenschutzreferent im niederländischen Justizministerium, später Präsident der niederländischen Datenschutzkommission und heute Europäischer Datenschutzbeauftragter, referierte u.a. über das UNO-Projekt von „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien", die am 14. Dezember 1990 von der UNO-Generalversammlung angenommen wurden. Ein Vorschlag des „Workshops New Media" zu Grundsatzfragen der Telekommunikation wurde verabschiedet und gleichzeitig der Grundstein für die Fortführung der Arbeit in der Form der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation gelegt.

Und am wichtigsten: Erstmals trafen sich die Datenschutzbeauftragten der Europäischen Gemeinschaft zu einer eigenen Sitzung und verabschiedeten eine „Zusatzerklärung der Datenschutzbeauftragten der EG-Länder". Sie forderten die Europäische Gemeinschaft und ihre Mitgliedstaaten auf, „in ihre Planungen … die Notwendigkeit eines umfassenden und konsistenten Ansatzes zur Verwirklichung der Grundsätze des Datenschutzes in der Mitgliedsländern und in bezug auf die Aktivitäten der Gemeinschaft selbst einzubeziehen". Die französische Datenschutzkommission wurde gebeten, diese Vorschläge „alsbald dem Vorsitzenden des Ministerrats sowie den Präsidenten des Europaparlaments und der EG-Kommission zu unterbreiten und um Unterstützung zu werben". Es war die Geburtsstunde der Europäischen Datenschutzrichtlinie.

Der Präsident der französischen Datenschutzkommission Jacques Fauvet, befreundet mit dem Präsidenten der EG-Kommission Jacques Delors, unterbreitete diesem persönlich das Konferenzanliegen. Im gleichen Jahr begannen die Beamten der Kommission mit den ersten Arbeiten an der Richtlinie.

Die Telekommunikation wird integriert und digitalisiert

Nach langen Vorbereitungen führte die Deutsche Bundespost 1989 das Dienste integrierende digitale Fernmeldenetz (Integrated Services Digital Network – ISDN) ein. Zunächst ging es um die Installation auf postinternen, vor allem überregionalen Netzebenen. Der Anschluss digitaler Endgeräte beim Verbraucher sollte erst später erfolgen. Mit dem Datenschutz bei ISDN stand die Deutsche Bundespost damals auf dem Kriegsfuß. Das informationelle Selbstbestimmungsrecht sollte gegenüber den Plänen der Bundespost, die für die Gebührenabrechnung erforderlichen Verbindungsdaten längerfristig für betriebsinterne Auswertungen zu speichern, zurückstehen. Ein Datenschutzkonzept für ISDN gab es

nicht, so dass wie erwähnt die Internationale Konferenz der Datenschutzbeauftragten sich veranlasst sah, weltweit geltende Anforderungen zur Datensparsamkeit und zur Datensicherheit bei ISDN zu formulieren.

Gleichzeitig mit der Digitalisierung der Backbone-Netze der Bundespost verbreitete sich die Digitalisierung hausinterner Telefonsysteme zu ISDN-fähigen Nebenstellenanlagen. Neu war, dass Telekommunikationsvorgänge unbemerkt aufgezeichnet und einzelnen Personen zugeordnet werden konnten, so dass Benutzerprofile entstanden. Telefongespräche konnten leichter unbemerkt mitgehört werden, persönliche Gespräche in Räumen konnten mittels manipulierter Freisprecheinrichtungen belauscht werden. Die neuen Risiken für angeschlossene Rechner waren ebenso problematisch wie die Bedeutung sicherer und vertrauenswürdiger Administration und Wartung für die anwendenden Behörden. Eine Prüfung in einem Eigenbetrieb zeigte, dass die Befürchtungen keineswegs aus der Luft gegriffen waren.

1990

Das Erbe der DDR

Die gescheiterte Idee der Kennedy-Administration anfangs der 60er Jahre, eine zentrale Einwohnerdatenbank der US-Bürger einzuführen, führte zu heftigen Diskussionen im amerikanischen Kongress und zur Forderung nach einem „Privacy Act“, in dem die Rechte des Staates zur Sammlung und Verarbeitung von Daten über seine Bürger begrenzt werden sollten. Es war der Beginn einer weltweiten Debatte, zu der die Deutschen mit dem missverständlichen, aber inzwischen in allen Sprachen verwendeten Wort „Datenschutz“ (data protection, protection des données, saschtschyta datych …) beitrugen. Trotz dieses Hintergrunds hatte auch die Bundesregierung versucht, eine „Bundesdatenbank“ aufzubauen, in der ähnlich den amerikanischen Plänen eine Personenkennzahl das zentrale Ordnungsmerkmal sein sollte. Sie scheiterte ebenfalls am Parlament: Der Rechtsausschuss des Bundestages kam zu der Auffassung, dass die Pläne verfassungswidrig seien – was das Bundesverfassungsgericht im Volkszählungsurteil bestätigte.

Die DDR hingegen griff – allerdings vor der Bevölkerung verborgen – die Idee auf und installierte eine umfassende Personendatenbank (PDB), die der zentralen

Speicherung von Daten für die Schutz- und Sicherheitsorgane der ehemaligen DDR diente und zur Deckung des Informationsbedarfs anderer Staatsorgane, staatlicher Stellen und gesellschaftlicher Einrichtungen gedacht war. Kern war das Zentrale Einwohnerregister (ZER), in dem sämtliche Meldedaten der 16 Millionen DDR-Bürger gespeichert und verarbeitet wurden. In der PDB wurden Strafregister der Generalstaatsanwaltschaft, Daten zur Kader- und Personalverwaltung, Reiseanträge, Daten der nationalen Volksarmee, aber auch Ausreisesperren, Führerscheinentzüge, Zugehörigkeit zu bewaffneten Organen, Sommerwohnungen, Waffenscheine und vieles mehr festgehalten. Gesetzliche Regelungen fehlten, datenschutzrechtliche Regelungen ohnehin. So gab es weder Zulässigkeitsvoraussetzungen noch Vorschriften zur Auskunft, Sperrung, Benachrichtigung und Löschung. Grundlage war lediglich ein Ministerratsbeschluss.

Für jeden Bürger wurde eine Personenkennzahl vergeben, unter der er in den Datenbeständen gespeichert war. Diese „PKZ“ begleitete den Bürger in sämtlichen Lebenssituationen.

Der Einigungsvertrag bestimmte, dass die neuen Länder innerhalb eines Jahres nach Wirksamwerden des Beitritts das Melderecht nach den Vorschriften des Melderechtsrahmengesetzes zu gestalten hatten. Melderechtsfremde Daten – insbesondere Ordnungsnummern – durften bis spätestens 31. Dezember 1992 weiterverwendet werden, solange sie für die Weiterführung des Melderegisters erforderlich waren. Ebenfalls zum frühestmöglichen Zeitpunkt, spätestens bis zum 31. Dezember 1992, waren sie an die Datenbestände der jeweiligen Fachverwaltungen zu überführen und danach im ZER unverzüglich zu löschen. Weiterhin waren sämtliche nach PKZ geordnete Dateien nach anderen Merkmalen umzuordnen. PKZ waren in allen Dateien zum frühestmöglichen Zeitpunkt zu löschen.

Die Umsetzung dieser Vorgaben gestaltete sich schwierig. Wegen des personellen Ausblutens des ZER war die ordnungsgemäße Abwicklung der Aufgaben, insbesondere die Übergabe der Meldedaten an die Kommunen, sehr gefährdet. Als wir eine Prüfung durchführten, wurden erhebliche Mängel erkennbar. Es stand nur noch ein qualifizierter Programmierer für alle notwendigen Arbeiten zur Verfügung. Das Landeskriminalamt hatte über das Landeskriminalamt Brandenburg einen unzulässigen Onlinezugriff auf die gesamten Meldedaten der fünf neuen Länder und Berlins. Dies hätte nur noch bei den örtlichen Meldebehörden nach Maßgabe des jeweiligen Landesmeldegesetzes erfolgen dürfen.

Datensätze sind weiter mit der PKZ geführt worden. Selbst für Neugeborene in den neuen Ländern wurde weiterhin eine PKZ vergeben. Das ZER hatte keine Löschung der PKZ bzw. der Umordnung nach einem anderen Ordnungsmerkmal

vorgenommen, weil das einen erheblichen programmtechnischen Aufwand bedeutet hätte, der angesichts der Personalsituation ein hohes Risiko für die Datenübergabe an die Landesmeldebehörden bedeutet hätte.

Die Meldestellen in den östlichen Bezirken Berlins arbeiteten noch mit den alten Meldekarten, die melderechtsfremde Daten, vor allem die verfassungswidrige PKZ, enthielten. Dadurch waren unzulässige Verknüpfungen mit anderen Karteien oder Dateien und damit rechtswidrige Nutzungen möglich. Uns wurde mitgeteilt, dass die Karteikarten in einigen Meldestellen noch bis 1997 erforderlich sind, da dort die Einführung der notwendigen EDV-Geräte früher nicht möglich ist. Selbst eine anlassbezogene Schwärzung der melderechtsfremden Daten hielt der Senat für zu kostenintensiv. Erst Mitte 2000 – mehr als zehn Jahre nach dem Mauerfall – wurde die letzte Meldestelle an das System angeschlossen.

1991

Datenverarbeitung in der Steuerverwaltung

Ein Finanzbeamter erblickt aus seinem Bürofenster eine junge hübsche Dame, die gerade aus ihrem Auto steigt, verbindet sich von seinem Arbeitsplatzsystem mit dem Datenbestand des für KfZ-Steuern zuständigen Finanzamts, erfährt so Namen und Adresse der Dame und nimmt mit ihr Kontakt auf. Da ihr dies nicht gefiel, erfuhren wir von dem Ereignis und begannen, uns für die Zugriffsregelungen und Zugriffsprotokollierungen bei den Systemen der Steuerverwaltung zu interessieren.

Das noch heute in Betrieb befindliche Verfahren DCL (Dezentrale Computerleistung in den Finanzämtern) wurde in einem dreistufigen Rechnernetz betrieben: Die Sachbearbeiter arbeiteten an Arbeitsplatzrechnern (PCs), die mit einem Finanzamtsrechner verbunden waren, der seinerseits mit dem zentralen Rechenzentrum der Finanzbehörden in Verbindung stand. Entsprechend waren auch die Zugriffsberechtigungen dreistufig vergeben, für die PC-Ebene, die Finanzamtsrechner und den Zentralrechner. Die Oberfinanzdirektion erließ eine Anweisung zur Differenzierung der Zugriffsberechtigungen, in der es den einzelnen Finanzämtern überlassen wurde, den Mitarbeitern die als notwendig erachteten Zugriffsberechtigungen einzuräumen. Normalerweise darf ein Finanzbeamter nur die

Daten seines eigenen Finanzamtes abfragen, aber auch finanzamtsübergreifende Abfragen waren möglich, zum Beispiel bei den KfZ-Speicherkonten des Finanzamts für Erbschafts- und Verkehrssteuern und bei Amtshilfeersuchen im Vollstreckungsbereich. Da solche Zugriffe der gegenseitigen Aufrechnung von Guthaben und Schulden in verschiedenen Steuerarten dienten, hatte prinzipiell jeder Sachbearbeiter die Möglichkeit des finanzamtsübergreifenden Zugriffs, auch auf die KfZ-Daten hübscher Frauen.

Wenn Zugriffsberechtigungen auf Grund dienstlicher Erfordernisse an viele Mitarbeiter vergeben werden, muss wenigstens dafür gesorgt werden, dass unbefugte Zugriffe im Nachhinein ruchbar werden können. Daraus ergeben sich Anforderungen an automatisierte Protokolle und ihre Auswertung. Da die Finanzbehörde ein besonderes Vertrauen in die Rechtschaffenheit ihrer Bediensteten hatte, begnügte sie sich jedoch im Vorgriff auf eine damals noch im Entwurf befindliche Steuerdatenabrufverordnung mit einer 5 %-Stichprobe bei finanzamtsübergreifenden Zugriffen. Es wurde nur jeder zwanzigste Abruf protokolliert. Der verliebte Finanzbeamte hatte also gute Chancen, dass sein Tun unbemerkt blieb, zumal er von der Protokollierung informiert wurde. Mit der Information über den Protokolleintrag hatte der Beamte lediglich den Grund des Abrufs in ein Buch einzutragen. Die Innenrevision verglich dann später die Protokolleintragungen des Abrufs mit den Eintragungen in dem Buch.

Wir haben festgestellt, dass die Wirksamkeit eines solchen Protokollierungsverfahrens zur Abschreckung unbefugter, weil zweckfremder Abfragen sehr beschränkt ist. Da der Bedienstete wegen der Unterrichtung damit rechnen muss, dass er sich für die Abfrage rechtfertigen muss, kann er einen dienstlichen Zusammenhang nachträglich konstruieren. So war es auch nicht verwunderlich, dass die Innenrevision bis zum Zeitpunkt der Prüfung noch keine Beanstandungen aussprechen musste.

1992

Datenschutz nun auch im Polizei- und Ordnungsrecht

1992 sind mit der Neufassung des Allgemeinen Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (ASOG) auch in Berlin ausdrückliche

Rechtsgrundlagen für die Informationsverarbeitung der Sicherheits- und Ordnungsbehörden geschaffen worden. Allerdings hätten wir uns gewünscht, wenn den Eingriffen in das Recht auf informationelle Selbstbestimmung engere Grenzen gesetzt worden wären.

Zentraler Gegenstand der Diskussionen war die Frage, in welchem Umfang personenbezogene Daten zur vorbeugenden Straftatenbekämpfung gespeichert werden dürfen. Das bisherige ASOG hatte hierauf keine Antwort gegeben.

Die Erhebung personenbezogener Daten zur vorbeugenden Straftatenbekämpfung wurde auf Straftaten von erheblicher Bedeutung beschränkt. Es wird nunmehr der Grundsatz hervorgehoben, dass die Verarbeitung vorhandener Daten zur vorbeugenden Straftatenbekämpfung nur Personen betreffen darf, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten begehen werden.

Bei Befragungen ist nunmehr der Betroffene nicht nur auf sein Verlangen, sondern von Amts wegen auf die Rechtsgrundlage und eine bestehende Auskunftspflicht oder die Freiwilligkeit seiner Eingaben hinzuweisen, allerdings nur, wenn dies die polizeilichen Aufgaben nicht erheblich erschwert oder gefährdet.

Daten von Personen, die in Gefahrenfällen Hilfe leisten („Gefahrenhelfer", z. B. Ärzte), können nur noch mit Einwilligung der Betroffenen verarbeitet werden. Die Voraussetzungen für die Ausschreibung zur polizeilichen Beobachtung, also die Erhebung von Daten über die Bewegung von Verdächtigen vor allem mit Kraftfahrzeugen, wurden verschärft. Diese Maßnahme darf nur eingesetzt werden bei gefährlichen Intensivtätern, bei denen weitere Straftaten zu erwarten sind.

Das ASOG dehnte nunmehr ausdrücklich die Polizeibefugnisse auf „andere Personen" aus. Damit wurde das hergebrachte Prinzip aufgegeben, polizeiliche Angriffe, außer in den Fällen des Notstandes, nur gegen Störer zuzulassen. Zur vorbeugenden Straftatenbekämpfung werden bis zu dreijährige Speicherungen der Daten von Personen ermöglicht, die sich keiner Straftat verdächtigt gemacht haben und nicht als Störer in Erscheinung getreten sind. Immerhin haben wir mit der Senatsverwaltung für Inneres Einigkeit erzielen können, dass die Speicherung der Daten dieses Personenkreises an besonders strenge Voraussetzungen zu knüpfen ist. So kann die Speicherung der Daten von Prostituierten künftig nicht mehr damit begründet werden, dass ihre Tätigkeit in einem Umfeld erfolgt, das nach polizeilicher Erfahrung erheblichen kriminellen Einflüssen ausgesetzt ist. Die für andere Personen vorgesehene Speicherfrist hat darüber hinaus dazu geführt, dass die bisher für fünf Jahre vorgesehene Registrierung der Prostituierten der Kartei

„Zuhälterei, Menschenhandel u. ä. Delikte“ erheblich verkürzt wurde und Datenlöschungen vorgenommen wurden.

Über die Auslegung des Gesetzes gab es auch gleich erste Meinungsverschiedenheiten. Die wichtigste betrifft den Umfang der Speicherung und Nutzung der Daten tatverdächtiger Personen. Die Polizei darf die zur Strafverfolgung erhobenen Daten nur speichern, soweit dies hierfür erforderlich ist. Nach Abschluss des jeweiligen Ermittlungsverfahrens sind die Daten damit grundsätzlich zu löschen. Eine weitere Speicherung dieser Daten ist aus unserer Sicht nur zulässig, soweit in jedem Einzelfall konkrete Tatsachen vorliegen, die die Annahme rechtfertigen, dass die Speicherung der Daten der betroffenen Person zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Die Polizei lehnte dies als zu weit gehend ab. Welche Voraussetzungen statt dessen berücksichtigt werden sollen, war nicht ersichtlich. Die Tatsache, dass es sich um einen Tatverdächtigen handelt, sollte offenbar schon ausreichen. Vielmehr müssen weitere konkrete Umstände hinzukommen, die die Erforderlichkeit und insbesondere Geeignetheit der Speicherung der Daten zur Bekämpfung künftig zu erwartender Straftaten belegen. Diese Voraussetzungen wurden vom Bundesverwaltungsgericht für die Aufbewahrung von erkennungsdienstlichen Unterlagen bereits 1983 entwickelt und können auf andere Datenspeicherungen zur vorbeugenden Straftatenbekämpfung übertragen werden.

1993

Olympiabewerbung: auch mit dem Datenschutz haperte es

Schon 1992 hatten wir uns mit der später eher kläglich gescheiterten Bewerbung Berlins um die Olympischen Spiele 2000 zu befassen. Zeitungen hatten berichtet, dass eine eigens für die Bewerbung gegründete Gesellschaft unzulässige Daten über die Mitglieder der IOC-Prüfungskommission sammelte. Tatsächlich stellten wir fest, dass für den Besuch der Kommission im Jahr 1993 Angaben über die Gästebetreuung vorhanden waren („trinkt gerne Bier“, „benötigt besonders großes Bett“ u. Ä.). Gerade noch kein Verstoß gegen das Bundesdatenschutzgesetz,

da tatsächlich ein Bezug zur gastfreundlichen Betreuung vorlag und keine Anhaltspunkte für von der Presse vermutete Bestechungsversuche zu finden waren.

Der Besuch fand im April 1993 statt. Die Begrüßung durch die Bevölkerung war allerdings nicht so freundlich, wie man sich das vorgestellt hatte: Demonstrierende Volkszählungsgegner waren nicht zu übersehen. Diese meinten, Berlin hätte in den neunziger Jahren Besseres zu tun als eine Olympiade vorzubereiten.

Vorsorglich war auf Veranlassung des polizeilichen Staatsschutzes bei über 200 Personen ein Hinweis in das Polizeiinformationssystem ISVB eingetragen worden, dass bei der Feststellung der Personalien sofort eine bestimmte Stelle anzurufen sei. Dieser Hinweis erschien bei jedem Aufruf auf dem Bildschirm. Abfrageberechtigt war fast jeder Berliner Polizist, der bei jedem Anlass, wie etwa einer Verkehrskontrolle, Kenntnis von dem gesteigerten Interesse des Staatsschutzes bekam.

Die Innenverwaltung billigte dies. Sie meinte, bei diesem Merker handele es sich lediglich um einen arbeitstechnischen Hinweis ohne Personenbezug, mit dem nur eine „Zuständigkeitsregelung“ zur weiteren Bearbeitung des Vorgangs getroffen werde. Das war natürlich abwegig: Der Abruf erweckte die durchaus beabsichtigte Vorstellung, dass der Betroffene ein militanter Gegner der Bewerbung von Berlin für die Olympischen Spiele im Jahr 2000 sei und sich der Staatsschutz deshalb für die Person interessiert. Eine solche Anprangerung ohne Anhaltspunkt für eine Straftat oder eine Gefahrensituation war und ist rechtswidrig.

Unbeschadet der fehlenden Rechtsgrundlage haben wir stichprobenweise überprüft, ob die Vergabe der Hinweise den eigenen Kriterien der Polizei entsprochen hat. Es fanden sich in keinem der untersuchten Fälle schriftliche Belege über die Gründe, die zur Vergabe des Hinweises bei den jeweiligen Betroffenen geführt haben. Eine Überprüfung der kriminalpolizeilichen Daten ergab, dass es bei diesen Personen allenfalls zu geringfügigen Straftaten wie Sachbeschädigung (z. B. Farbschmierereien, Abreißen oder Ankleben von Plakaten), Beleidigungen (z. B. das In-die-Höhe-Strecken des rechten Armes und des Mittelfingers gegen Polizeibeamte, wobei der Beschuldigte unter erheblichem Einfluss von Alkohol stand), Diebstahl (z. B. von Fahnen und Aufklebern) und Hausfriedensbruch kam.

Wir haben darüber hinaus wiederum festgestellt, dass die Daten von über 100 Personen auch in der PIOS-Datei des BKA gespeichert wurden. Die zur Terroristenbekämpfung eingerichtete Datei entwickelte sich offensichtlich zu einer Datei für politisch – vielleicht in etwas überschießender Weise – motivierte Aktivisten,

auch wenn diesen erhebliche, bundesweit relevante Straftaten nicht nachzuweisen waren. Volkszählungsgegner, Olympiagegner – zehn Jahre später waren es Globalisierungsgegner, die ein Transparent gegen das Abholzen der Regenwälder in Brasilien entrollten.

Zeitungen meldeten, dass kurz vor der Entscheidung über den Austragungsort in Monaco im September 1993 Fotos von mehreren Hundert Olympiagegnern in das Fürstentum übermittelt worden sein sollen. Weiterhin soll bei Überprüfungen von Personen durch die monegassische Polizei – offenbar durch vor Ort anwesende Berliner Polizeibeamte – ein Datenabgleich mit den Beständen der Berliner Polizei erfolgt sein. Tatsächlich waren Berliner Polizeibeamte nach Monaco entsandt werden. Zu ihrer eigenen Verwendung hatten die Berliner Beamten 133 Lichtbilder und 164 Personendatensätze von Personen, die als gewaltbereite Olympiagegner eingestuft waren, dabei. Über Interpol und das BKA fragte die monegassische Polizei aber auch selbst Daten über mehr als hundert Personen und Kraftfahrzeuge ab – die datenschutzrechtliche Überprüfung der Vorgänge erwies sich als langwierig und unbefriedigend.

1994

QuasiNiere, nach schwieriger Geburt ein langes Leben

Bei QuasiNiere muss immer alles von einem Tag auf den anderen erledigt werden. Manches dauert aber eben doch länger, so wie unsere mittlerweile zehnjährige Begleitung, Prüfung und Kontrolle des Qualitätssicherungsprojektes in der Nierenersatztherapie – QuasiNiere. Mitte 1994 ein Anruf – man möchte da eben mal für ein Qualitätssicherungsprojekt alle Praxen und Einrichtungen in Deutschland, die Dialyseleistungen anbieten, befragen. Dazu hatte man aus Telefon- und Adressbüchern fast 1.000 medizinische Einrichtungen herausgefiltert. Wir prüften den Erhebungsbogen, gaben einige Hinweise und zwei Tage später konnte der Versand beginnen. Dann ein weiterer Hilferuf von QuasiNiere. Das Projekt war in

den ersten drei Jahren der Ärztekammer Berlin angegliedert. Der Geschäftsführer der Ärztekammer war der Auffassung, dass die von den Einrichtungen zurückgesandten Erhebungsbögen über deren Leistungen, Anzahl und Art der Patienten usw. selbstverständlich erst ihm geöffnet zur Kenntnis zu geben sind. Nicht ganz ohne Druck fand sich dann aber schließlich ein Einsehen, dass QuasiNiere eine eigenständige Daten verarbeitende Stelle ist und die Ärzte nur dieser und nicht der Ärztekammer die Daten über ihre Einrichtungen liefern wollen, wie es ihnen auch schriftlich zugesichert wurde.

QuasiNiere war eines von zehn Projekten des Bundesgesundheitsministeriums zur Qualitätssicherung in der medizinischen Behandlung, die nach dem Gesundheitsreformgesetz 1992 ins Leben gerufen wurden. Mittlerweile hat es als einziges Projekt überlebt und gilt nicht zuletzt wegen der Organisation des Datenschutzes als beispielhaft. Da QuasiNiere in der zweiten Stufe nicht nur als Einrichtungs-, sondern auch als Patientenregister ausgebaut wurde, kostete es uns einige Anstrengungen, die Expertengruppe von Ärzten davon zu überzeugen, dass trotz der Einwilligung der Patienten das Register selbst keine personenbezogenen, sondern nur pseudonymisierte Daten verarbeiten sollte. Dazu wurde als Datentreuhänder ein Notar verpflichtet, der nunmehr mittels modernster Technik die Klarnamen der Patienten und die Pseudonyme verwaltet, während das Register selbst nur die medizinischen Daten von derzeit ca. 80.000 Patienten unter Pseudonym verarbeitet.

QuasiNiere gelang es immer wieder, für den zuständigen Referenten eindrucksvolle Termine zu finden. So fand 1995 die grundlegende Besprechung, während der das Datentreuhändermodell endgültig auch von der Expertengruppe des Projekts bestätigt wurde, eine Stunde nach einem Termin des Referenten beim Familiengericht statt. Für die Jahrestagung des kontrollierenden Beirats 2003 wählte QuasiNiere den Hochzeitstermin des Referenten, sodass dieser noch Gelegenheit hatte, auf dem Rückweg von der Sitzung den entscheidenden Blumenstrauß zu kaufen.

Dass es bei der Begleitung, Prüfung und Kontrolle des Projektes nicht immer nur trocken zuging, bewies unser gemeinsamer Stand bei der „Langen Nacht der Wissenschaften“ am 13. Juni 2004. QuasiNiere schenkte an die ca. 4.000 Besucher in der Glashalle des Virchow-Klinikums zwei Arten von kleinen Drinks aus, den Pseudomeiser und den Anomeiser. Somit konnten wir gemeinsam den Besuchern erklären, dass bei reichhaltigstem Genuss des Anomeisers Name, Wohnanschrift u. Ä. für Stunden, wenn nicht für immer verloren gehen, während der vitaminreiche Pseudomeiser die Gedächtnisleistung und die Speicherkapazitäten der Besucher in keiner Weise beeinträchtigte.

1995

Das Begrüßungspaket: Die BahnCard

Direkt nach der Übernahme der Aufgaben der Aufsichtsbehörde am 1. August 1995 hatten wir ein Problem zu lösen, welches mehrere Wochen die Öffentlichkeit beschäftigt hatte, nämlich die datenschutzrechtliche Bewertung der neuen BahnCard.

Bei der neuen Karte, die wie bisher zum Kauf einer Fahrkarte zum halben Preis berechtigte, hatten die BahnCard-Kunden die Möglichkeit, zwischen drei Varianten zu wählen, nämlich der BahnCard Pur, der BahnCard mit Kreditkartenfunktion und dem Angebot einer Elektronikguthabenkarte. Bei der Erstellung der Formulare hatte die Deutsche Bahn AG den Fehler begangen, Daten, die sie nur bei Kartenkunden mit Zusatzfunktion benötigte, auch bei BahnCard-Pur-Kunden abzufragen. Dieser Fehler konnte durch ein neues Formular mit optisch getrennten Bereichen für die jeweiligen BahnCard-Typen ohne große Schwierigkeit gelöst werden.

Die Mehrzahl der Bürgereingaben betraf aber die bei dem neuen BahnCard-Verfahren vereinbarte Zusammenarbeit zwischen der Deutschen Bahn AG und der Citibanktochter Citicorp Card Operations GmbH, die die Karten in einem Rechenzentrum der Citibank in den USA herstellte, also in einem Land, welches nach wie vor über kein ausreichendes Datenschutzniveau verfügt. 1995 enthielt das Bundesdatenschutzgesetz noch keine Regelungen für Datenflüsse über die Grenzen Deutschlands und Europas hinaus.

Da es nicht unsere Aufgabe sein konnte, der Deutschen Bahn AG Vorgaben bezüglich ihrer Kooperationspartner zu machen, mussten wir mit ihr und der Citibank Vorgaben entwickeln, die das geplante Vorhaben datenschutzrechtlich absicherten.

Die von uns geforderten Modalitäten führten zu der vielleicht ersten datenschutzgerechten Datenübermittlung in ein Land ohne ausreichendes Datenschutzniveau. Das vereinbarte Verfahren wäre auch nach der novellierten Fassung des Bundesdatenschutzgesetzes rechtmäßig, da durch Vertragsklauseln ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gewährt wurden. Die Citibank hat sich vertraglich ver-

pflichtet, auch bei der Datenverarbeitung in den USA das deutsche Datenschutzniveau nicht zu unterschreiten. Insbesondere hat sie sich verpflichtet, Daten von BahnCard-Kunden nur in engen Grenzen für Marketingzwecke zu nutzen. Kunden von der BahnCard Pur durften von der Citibank überhaupt nicht beworben werden. Die Citibank unterwarf sich für das BahnCard-Verfahren – auch bezüglich des Rechenzentrums in den USA – der Kontrolle unserer Behörde. Uns wurde die Möglichkeit eingeräumt, vor Ort selbst Datenschutzprüfungen vorzunehmen bzw. durch Beauftragte vornehmen zu lassen. Außerdem wurde den BahnCard-Kunden das Recht eingeräumt, Ansprüche auf Auskunft, Löschung, Sperrung oder Schadensersatz sowohl gegenüber der Deutschen Bahn AG als auch gegenüber der Citibank geltend zu machen.

Auch im Knast gibt es informationelle Selbstbestimmung

1994 fand in der Justizvollzugsanstalt Tegel eine der umfangreichsten Prüfungen statt, die wir bisher durchgeführt haben. Drei Wochen lang besuchten mehrere Mitarbeiterinnen und Mitarbeiter die verschiedenen Teile der mit etwa 1.500 Strafgefangenen einer der größten Strafvollzugsanstalten Deutschlands. Es gab noch keine datenschutzrechtlichen Vorschriften im Strafvollzugsgesetz und die hohe Anzahl an Eingaben und Beschwerden von Gefangenen aus den Berliner Justizvollzugsanstalten ließ sich datenschutzrechtlich nur schwer bewerten.

Wir prüften die Vollzugsgeschäftsstelle, die Teilanstalten, dort Hausbüros mit Gefangenenpersonalakten, die sozialtherapeutische Anstalt, die Arbeitsverwaltung, Werkstätten der Justizvollzugsanstalt, die pädagogische Abteilung, die Arztgeschäftsstelle, den zahnärztlichen Dienst, die Hauskammern einiger Teilanstalten, die sozialpädagogische Abteilung, das Fotostudio, die Telefonzentrale, das Tor sowie verschiedene Archive. Da die Justizvollzugsanstalt Tegel aus mehreren Teilanstalten besteht, mussten zahlreiche Stellen auch in mehreren Teilanstalten geprüft werden. Es ist leicht vorstellbar, dass bei einer über drei Wochen andauernden Prüfung in einem so sensiblen Bereich wie dem Strafvollzug auch der Prüfbericht am Ende einen entsprechenden Umfang aufweist. Es waren immerhin fast 300 Seiten Prüfbericht. Einige im Prüfbericht immer wiederkehrende Probleme waren die Aufteilung der Gefangenenpersonalakten im Hinblick auf die Zugriffsrechte Dritter und die damit verbundenen Akteneinsichtsrechte, das Nichtvorhandensein von Aufbewahrungsvorschriften für eine Vielzahl von Datensammlungen und auch Doppelspeicherungen, die aufgrund der vielfältig geführten Dateien entstanden sind. Die Prüfung hat alle an ihr beteiligten Stellen über einen langen Zeitraum beschäftigt. Die Nacharbeit hat über viele Jahre angedauert.

Die Prüfung war allerdings ein großer Erfolg, weil sie die Mitarbeiter im Bereich des Strafvollzugs für datenschutzrechtliche Fragen sensibilisiert hat und es zu zahlreichen Verbesserungen innerhalb des Strafvollzuges gekommen ist. Die 1998 in Kraft getretene Änderung des Strafvollzugsgesetzes hat dann auch durch die Aufnahme datenschutzrechtlicher Regelungen viele Probleme, auf die wir gestoßen waren, gesetzlich geregelt und damit gelöst.

1996

Die Führerscheinakte – ein lebenslanges Sündenbuch?

Die Unterlagen, die in den Führerscheinakten früher beim Polizeipräsidenten, seit 1986 im Landeseinwohneramt von allen Personen aufbewahrt werden, die in Berlin ihren Führerschein gemacht haben, sind von Anfang an von uns kritisch beäugt worden. Strafurteile, auch wenn sie nichts mit Verkehrsdelikten zu tun hatten, wurden ungeachtet der Tilgungsfristen des Bundeszentralregistergesetzes lebenslänglich aufbewahrt. Für medizinisch-psychologische Untersuchungen („Idiotentests“) angefertigte Gutachten mit sensiblen Daten wurden ebenso uneingeschränkt abgeheftet wie denunzierende Mitteilungen von Nachbarn („der hatte einen Schlaganfall und fährt immer noch Auto“).

Die Frage, ob diese Akten komplett an Gutachter übermittelt werden dürfen oder vielmehr vorher auf relevante Teile durchgesehen werden müssten, führte zu einer umfassenden Prüfung. Es wurden stichprobenartig Erstanträge auf Erteilung einer Fahrerlaubnis, Neuerteilungen, bestehende Führerschein- und Personenbeförderungsakten durchgesehen.

Die Straßenverkehrsvorschriften enthielten noch keine Regelungen über die Aufbewahrungsdauer von Unterlagen in den Führerscheinakten. Für die datenschutzrechtliche Bewertung konnten daher nur die allgemeinen Bestimmungen des Allgemeinen Sicherheits- und Ordnungsgesetzes herangezogen werden. Danach konnten Ordnungsbehörden Daten nur dann verarbeiten, soweit das zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Der Grundsatz der Erforderlichkeit beschränkt die Speicherung auch in zeitlicher Hinsicht.

Sowohl in den Vorgängen zur Ersterteilung als auch in den Akten zur Neuerteilung von Fahrerlaubnissen waren Unterlagen enthalten, die den genannten Erforderlichkeitskriterien nicht entsprachen. Festgestellt wurden u. a. Führerscheinkarteikarten der ehemaligen DDR mit Personenkennzahl, Führungszeugnisse für Behörden, Anklageschriften und Urteile von Strafgerichten ohne Bezug zum Straßenverkehr, Ausfertigungen von Haftbefehlen und Anfragen zu Insassen von Justizvollzugsanstalten. Den Gutachtern in den medizinisch-psychologischen Untersuchungsstellen wurde tatsächlich die komplette Akte übersandt. Eine Prüfung dahingehend, ob der gesamte Akteninhalt für die Aufgabenerfüllung der Gutachter erforderlich ist, fand nicht statt. Wir beanstandeten diese Praxis.

Am 1. Januar 1999 trat eine umfassende Änderung des Straßenverkehrsgesetzes in Kraft, die die von den Datenschutzbeauftragten seit jeher erhobenen Forderungen umsetzte. Innerhalb von zehn Jahren müssen nunmehr die Akten bereinigt werden. Um diese Frist einzuhalten, forderte das Abgeordnetenhaus am 27. September 2001 den Senat auf, jährlich über die Umsetzung der neuen Vernichtungsfristen in der Führerscheinstelle zu berichten. Danach sind von 370.000 im Jahr 1999 vorhandenen Akten bis 2004 ungefähr 195.000, also mehr als die Hälfte, vernichtet oder bereinigt worden. Es besteht also gute Hoffnung, dass das Ziel erreicht wird.

1997

Der Spannungsbericht

Die Parteien der Großen Koalition wollten es wissen: Im April 1997 beschloss das Abgeordnetenhaus, dass der Senat einen Bericht darüber erstellen sollte, ob und gegebenenfalls in welchen Fällen im Bereich der Kriminalitätsbekämpfung ein „Spannungsfeld zwischen Datenschutz und schutzwürdigen Belangen der Allgemeinheit besteht“. Schon die Fragestellung zeugte von einem Missverständnis des Datenschutzes: Das Recht auf informationelle Selbstbestimmung, dessen Ausprägung der Datenschutz ist, hat Grundrechtsqualität und dient damit ebenfalls den „schutzwürdigen Belangen der Allgemeinheit“.

Polizei und Verfassungsschutz nutzten den Auftrag, ein allgemeines Lamento über die Bürden anzustimmen, die ihnen angeblich der Datenschutz im Allgemeinen

und der Datenschutzbeauftragte im Besonderen zumutet. Letzterem wurde vorgeworfen, er greife bei seinen Prüfungen „tief in rechtliche und fachliche Beurteilungskompetenzen der Polizei“ und anderer Behörden ein. Dabei muss bei der Kontrolle von Datenerhebungen, Speicherungen und Übermittlungen selbstverständlich geprüft werden, ob die Eingriffsvoraussetzungen vorliegen. Wenn diese weitgehend aus Generalklauseln bestehen und die Erforderlichkeit für die Aufgabenerfüllung das einzige von den Gesetzen vorgegebene Kriterium ist, muss sie eben vom Datenschutzbeauftragten beurteilt werden.

Die Wehklagen ließen kaum eine der datenschutzrechtlichen Pflichten aus. Das Recht der Betroffenen auf Auskunft und Akteneinsicht sowie auf Information über eine mehr als fünfjährige Speicherung (deren Dauer hinterher gegen unseren Protest verlängert wurde), die Pflicht zur Löschung von Daten und Bereinigung von Akten, die technisch-organisatorischen Maßnahmen zur Wahrung des Datenschutzes – alles behindere die Strafverfolgung. Der Bericht gipfelte in der Behauptung, 47 Mitarbeiter würden sich mit dem Datenschutz befassen – und verschwieg, dass sie dies wenn überhaupt nur zu einem geringen Teil ihrer Arbeitszeit tun.

Obwohl datenschutzrechtlich gegenüber der Polizei begünstigt, stimmte der Verfassungsschutz in das Klagelied ein. Die – selbstverständliche – Dokumentation von Datenübermittlungen, die Begründung bei der Ablehnung von Auskunftsanträgen, die Löschung (nicht) mehr erforderlicher Daten wurden als lästige und abschaffungswürdige Pflichten dargestellt.

Lediglich die Justizverwaltung räumte ein, dass stets angemessene Lösungen für datenschutzrelevante Sachverhalte gefunden werden konnten, und erkannte die Tätigkeit des Berliner Datenschutzbeauftragten als notwendig und hilfreich an.

Der Bericht wurde nach kurzer Diskussion im Unterausschuss Datenschutz des Abgeordnetenhauses ad acta gelegt.

Entsetzen über den Todescomputer

Schlagzeilen wie „Darf ein Computer über das Leben entscheiden“ oder „Der virtuelle Todesstoß“ beherrschten insbesondere die Boulevardpresse im Sommer 1997. Man hatte herausgefunden, dass in der Intensivstation der Charité ein Com-

puterprogramm namens „RIYADH“ für die Qualitätssicherung eingesetzt wurde. Die Befürchtungen waren groß, dass mit diesem Programm automatisch diejenigen Patienten aus der Intensivbehandlung herausgenommen würden, bei denen geringe oder keine Heilungschancen mehr bestehen. Ganz unbegründet war dies nicht: Das Programm war während des ersten Golfkrieges in der saudi-arabischen Hauptstadt entwickelt worden, um die Belegung von Lazaretten mit Verwundeten zu steuern.

Bei unserer Prüfung stellte sich allerdings heraus, dass diese Befürchtungen grundlos waren. Zwar wurden in der Tat Daten von Intensivpatienten in das Programm eingegeben und einem „Patientenscoring“ unterzogen. Dies geschah aber erst nach der Entlassung aus der Intensivstation. Das Personal, das die Daten eingab, arbeitete selbst nicht dort, die Daten wurden in pseudonymer Form eingegeben. Die Auswertungen wurden genutzt, um die Behandlungsmethoden zu bewerten und zu verbessern. In keinem Fall war daran gedacht, die Behandlung eines Patienten vorzeitig zu beenden, weil der Computer seine Überlebenschance als gering bewertet hat.

Gleichwohl zeigt der Fall, welche Ängste der Einsatz von Informationstechnik auslösen kann, auch wenn sie nicht gerechtfertigt sind.

1998

Die größte Niederlage: Der Große Lauschangriff

Das Bundesdatenschutzgesetz war drei Wochen zuvor verkündet worden, aber bisher nur teilweise in Kraft. Da meldete der Spiegel am 26. Februar 1977, der Atomwissenschaftler Günter Traube sei monatelang am Telefon abgehört worden, da er verdächtigt wurde, mit RAF-Terroristen in Verbindung zu stehen, und da er diesen möglicherweise sogar Nuklearmaterial verschaffen könnte. Nicht nur das:

Er sei auch in seiner Wohnung mit einem Mikrofon belauscht worden. Ein grober Verstoß gegen das Grundrecht auf Unverletzlichkeit der Wohnung. Eine Diskussion begann, ob ein derartiger Eingriff angesichts der Bedrohung durch den Terrorismus nicht zugelassen werden sollte. Angeblich war es ein Beamter des Bundeskriminalamtes selbst, der hierfür den inzwischen von den Sicherheitsbehörden verpönten Begriff „Großer Lauschangriff" prägte (im Gegensatz zum „Kleinen Lauschangriff", der Wanze, die ein Ermittler zum Eigenschutz bei sich trägt).

Gut 20 Jahre später war es so weit: Nunmehr diente die Organisierte Kriminalität als Argument dafür, das Grundgesetz zu ändern und den Großen Lauschangriff zuzulassen. Unter maßgeblicher Beteiligung des heutigen Bundesinnenministers wurde die notwendige Zweidrittelmehrheit im Bundestag sichergestellt. Die FDP-Justizministerin Sabine Leutheusser-Schnarrenberger trat nach einer parteiinternen Mitgliederbefragung, bei der sich die Mehrheit der Liberalen für den Lauschangriff entschied, von ihrem Amt zurück. Energische Äußerungen von Datenschutzbeauftragten und Appelle wie der „Bonner Appell gegen den geplanten Großen Lauschangriff" vom 5. März 1998, den 43 Institutionen unterstützten, halfen nichts. Am 26. März 1998 beschloss der Bundestag die notwendige Änderung des Artikel 13 Grundgesetz, die Anpassung der Strafprozessordnung folgte am 4. Mai 1998.

Der Große Lauschangriff wurde seither selten eingesetzt und wenn, dann mit wenig Erfolg. Technische Pleiten, unverständliche Sprachen, Schnarchgeräusche statt der erwarteten vertraulichen Informationen zeigten, dass der Aufwand und die Tiefe des Eingriffs in die Privatsphäre in keinem angemessenen Verhältnis zum eingetretenen Fahndungserfolg standen.

Die zurückgetretene Justizministerin wollte es zusammen mit anderen FDP-Politikern und engagierten Bürgern noch einmal wissen: Sie legten Verfassungsbeschwerde beim Bundesverfassungsgericht ein. Dies entschied nach einer mündlichen Verhandlung, in der auch alle Pannen zur Sprache kamen (der Verfassungsrichter Bryde: „Der Datenschutz wird offensichtlich durch technische Probleme gewährleistet"), am 3. März 2004, dass die Bestimmungen der Strafprozessordnung zum Großen Lauschangriff teilweise verfassungswidrig sind. Dem Menschen müsse ein Kernbereich privater Lebensgestaltung bleiben, bei dem eine Abwägung mit den Sicherheitsinteressen des Staates „nicht stattfindet".

Die nahe liegende Konsequenz, unter diesen Umständen auf den Großen Lauschangriff zu verzichten, wird wohl nicht gezogen. Im Bundesrat liegt derzeit ein Gesetzentwurf der Bundesregierung, mit dem die Vorgaben des Bundesverfas-

sungsgerichts umgesetzt werden sollen. Wenn es zu persönlich wird, müssen die Lauscher künftig abschalten – wonach sie beurteilen sollen, wann sie wieder hinhören dürfen, wird nicht geregelt.

Auch die Sozialamtsfalle wird Gesetz

Das Ereignis lag viele Jahre zurück. Nicht lange nach Inkrafttreten der Datenschutzbestimmungen des Sozialgesetzbuches im Jahr 1981 wurde ein Arbeitsloser zur Haft ausgeschrieben, weil er seiner Ehefrau in einer heftigen Auseinandersetzung die Handtasche weggenommen hatte, was die Staatsanwaltschaft als Raub qualifizierte. Als er wieder einmal im Arbeitsamt erschien, informierte eine Sachbearbeiterin die Polizei. Der Vorgesetzte, der hiervon hörte, schickte den Betroffenen weg. Dies trug ihm eine Strafanzeige wegen Strafvereitelung im Amt ein. Er wehrte sich unter Berufung auf das Sozialgeheimnis dagegen.

Strittig war der Begriff der „derzeitigen Anschrift“. Nach der damals geltenden Regelung im Sozialgesetzbuch waren Sozialleistungsträger berechtigt, diese Angabe an die Polizei herauszugeben. Obwohl niemand einen vernünftigen Zweifel daran haben konnte, was der Begriff „derzeitige Anschrift“ bedeutet, nämlich gerade nicht wo sich Personen soeben aufhalten, hatte das Berliner Kammergericht 1993 entschieden, dass der Begriff der „derzeitigen Anschrift“ als „Minus“ auch den „gegenwärtigen Aufenthalt“ umfasse. Der Vorgesetzte kam zwar wegen Verbotsirrtums um die Strafe herum. Aber das Problem selbst verfolgte uns jahrelang. Nur zu gerne wollte die Polizei Sozialleistungsempfänger in diese Falle locken.

Besondere Brisanz bekam das Problem bei der Frage der Behandlung illegal eingereister Ausländer, die Sozialleistungen in Anspruch nehmen wollten. Sollten Daten einer Rumänin, die ein hungriges Baby auf dem Arm hatte und um Lebensmittel bat, erhoben und an die Polizei zur Abschiebung übermittelt werden? Unsere zurückhaltende Auffassung hat uns den Vorhalt des Innensenators eingehandelt, wir würden die „Lunte an das Fass der Ausländerfeindlichkeit“ halten.

1998 war es dann auch so weit. An versteckter Stelle wurde im Medizinproduktegesetz vom 6. August 1998 ganz unverfänglich und überraschend der einschlägige Paragraph des Sozialgesetzbuches geändert. Nunmehr durfte auch der derzeitige oder zukünftige „Aufenthaltsort“ mitgeteilt werden. Die Fallenstellerei war legitimiert.

1999

20 Jahre nach dem Datenschutz auch Informationsfreiheit in Berlin

In dem Bericht zur Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten war schon darauf hingewiesen worden, dass dem Datenschutz das Recht auf Zugang zu den Informationen der Verwaltung an die Seite gestellt werden müsste. Zwanzig Jahre später war es so weit.

Seit dem 30. Oktober 1999 gilt in Berlin das Informationsfreiheitsgesetz (IFG), das jedem Menschen, aber auch Vereinen, Unternehmen und anderen juristischen Personen das Recht auf Akteneinsicht und -auskunft gegenüber den öffentlichen Stellen des Landes Berlin gewährt, ohne dass die Antragsteller ein besonderes Interesse vorbringen müssen. Damit hat Berlin als zweites Bundesland nach Brandenburg einen Meilenstein zu mehr Transparenz im Staat gesetzt. Ein leichtes Unterfangen war das keineswegs, geht dem Gesetz doch eine über zehnjährige Entstehungsgeschichte voraus. Ein erster Anlauf erfolgte bereits während der rotgrünen Koalition 1990, als die Fraktion der Alternativen Liste (die Vorläuferin der Fraktion Bündnis 90/Die Grünen) einen Gesetzentwurf in die parlamentarische Beratung eingebracht hatte (damals in die zwei Berliner Parlamente, das Abgeordnetenhaus im Westteil und die Stadtverordnetenversammlung im Ostteil der Stadt). Am Ende der Legislaturperiode standen die Grünen vor der Wahl, entweder ein IFG oder ein Landesgleichstellungsgesetz durchzusetzen. Dem fiel das IFG zum Opfer.

1997 brachte dann die in der Opposition stehende Fraktion Bündnis 90/Die Grünen den Gesetzentwurf erneut in das Abgeordnetenhaus ein. Die Initiative stieß auf erheblichen Widerstand in Politik und Verwaltung. Das lag weniger an dem Gedanken der Informationsfreiheit als Ausdruck einer transparenten Verwaltung. Vielmehr wurden pragmatische Argumente vorgebracht: Gewarnt wurde vor missbräuchlichen Anträgen mit dem Ziel, die Verwaltung lahmzulegen. Auch würde die Flut von Anträgen einen erheblichen Personal- und Kostenaufwand verursachen. Die Gegner des IFG, zu denen auch der Innensenator gehörte, gingen ganz offensichtlich davon aus, dass die Berliner Bevölkerung in Scharen die Rathäuser und Verwaltungsgebäude stürmen würde. Die Mehrheit des Parlaments ließ sich von diesem Schreckensszenario nicht blenden und verabschiedete das IFG in der letzten Sitzung der damaligen Legislaturperiode am 15. Oktober 1999 gegen die Stimmen der mitregierenden CDU.

Hauptmerkmal ist eine neue Gewichtung zwischen Datenschutz und Informationsfreiheit, die deutlich zugunsten der Informationsfreiheit erfolgte. Selbstverständlich hat auch der Schutz personenbezogener Daten im IFG seinen Niederschlag gefunden, wenn auch nicht in absoluter Form. So ist der Name des Amtsträgers, der an einer Verwaltungsentscheidung mitgewirkt hat, als personenbezogenes Datum alles andere als schützenswert. Wer in der eigenen Nachbarschaft in welcher Höhe Sozialhilfe erhält, ist dagegen nach wie vor nicht zu offenbaren, denn diese Informationen unterliegen dem Sozialgeheimnis. Andere Einschränkungen neben dem Datenschutz schützen die staatliche Entscheidungsfindung oder Geschäftsgeheimnisse.

Wir haben eine Vermittlerrolle zugesprochen bekommen. Die Koppelung der Kontrolle des Datenschutzes und der Informationsfreiheit bei einem Beauftragten ist sinnvoll und hat sich auch in Berlin bewährt. Zwar besteht zwischen Datenschutz und Informationsfreiheit ein natürliches Spannungsverhältnis. Beides ist aber Ausdruck der informationellen Selbstbestimmung und Grundlage für das eigenverantwortliche Handeln des Bürgers in der Informationsgesellschaft.

Die zwischenzeitlich gesammelten Erfahrungen zeigen, dass sich die Befürchtungen der Verwaltungen, sie würden mit einer Flut von Informationszugangsanträgen konfrontiert, die sie zu ihren eigentlichen Aufgaben nicht mehr kommen ließen, nicht bewahrheitet haben. Zumeist wird Informationszugang im Baubereich begehrt. Hier sind insbesondere Bürgerinitiativen bei großen Bauvorhaben aktiv. Auch Grundstücksgeschäfte und -bewertungen der öffentlichen Hand spielen eine herausragende Rolle. Lärmgeplagte Nachbarn von Biergärten begehrten Einsicht in die Gewerbeakten der Gaststätten. Ein Bürger wollte die Unterlagen zur öffentlichen Förderung eines Millionenprojekts einsehen. Weitere Einsichtsbegehren betrafen Baumgutachten, die Übersicht zu Gebäuden mit Ofen- und Ölheizung, Protokolle von Sitzungen der Zahnärztekammer, Hinweise für die Prüfer beim zweiten juristischen Staatsexamen, den Außenanstrich eines Rathauses usw. usw.

2000

Kontrollen in Berliner Krankenhäusern

Die Wahrung des Datenschutzes und damit auch der ärztlichen Schweigepflicht ist in den Krankenhäusern ein schwieriges Unterfangen, wie wir 2000 in zwei unterschiedlichen Kontrollen erfahren mussten.

Ein Problem ist zum Beispiel, wer Zugriff auf die Daten eines Patienten in medizinischen Dokumentationssystemen haben soll. Selbstverständlich sollen die behandelnden Ärzte den Zugriff haben, also etwa die Ärzte einer Abteilung, die sich auch gegenseitig vertreten und unterstützen. Konsiliarärzte benötigen den Zugriff, wenn ihr Rat im Einzelfall gebraucht wird. Ärzte mit klinikübergreifenden Aufgaben wie z. B. die Anästhesisten brauchen im Einzelfall den Zugriff. Auch für den Notfall muss der Zugang zu den Daten eines Patienten gesichert sein.

Im Campus Virchow der Charité, in der wir das Dokumentationssystem GUSTAV der chirurgischen Abteilungen und der Anästhesie prüften, hatte man es sich ganz einfach gemacht: Obwohl das System Zugriffsdifferenzierungen zuließ, wurde bestimmt, dass prinzipiell alle Ärzte dieser Abteilungen, auf Antrag Pflegepersonal, Studenten und Personen aus anderen Abteilungen Zugriff auf alle Patientendaten erhielten. Was aber gehen den Gynäkologen die Daten des Prostata-Kranken in der Chirurgie an? Eine solche pauschale Zugriffsregelung bricht die ärztliche Schweigepflicht und widerspricht den einschlägigen gesetzlichen Vorschriften.

Ein wenig besser sah es in einem anderen Dokumentationssystem im Campus Mitte der Charité aus. Dort beschränkte sich der Zugriff auf die Daten der Patienten einer Station, aber auch dort gab es für den Hygienedienst und die Anästhesie Zugriffsprivilegien, die nicht hinreichend begründbar waren.

Die Charité reagierte auf unsere Beanstandungen mit der Einschaltung eines externen Gutachters. Da dieser uns Recht gab, wurden Maßnahmen organisatorischer und programmtechnischer Art zur signifikanten Verbesserung des Schutzes der Patientendaten eingeleitet. Es wurde angekündigt, auch andere Systeme auf die Einhaltung der Anforderungen des Datenschutzes hin zu untersuchen.

Eine weitere Kontrolle betraf ein Klinikum des damals in Gründung begriffenen Vivantes-Konzerns, also einen früheren Krankenhausbetrieb eines Berliner Bezirkes. In Ermangelung eines durchgängigen Anwendungskonzepts für die Anwendungen der Informationstechnik machte jede Abteilung, was sie wollte, also ohne gegenseitige Abstimmung. Einige Abteilungen setzten ein Sicherheitskonzept um, anderen Abteilungen war die technische Sicherheit ihrer Systeme offensichtlich völlig egal. Räume, in denen IT-Systeme mit sensiblen Patientendaten in Betrieb waren, blieben unbewacht und unverschlossen, so dass nicht nur die Kontrolleure, sondern jeder Patient oder Besucher die Daten hätte einsehen, ja sogar die Datenverarbeitungsprozesse hätte manipulieren können.

Höhepunkt war der ungestörte Spaziergang durch unterirdische Katakomben von einer stets offen gehaltenen Tür vom Freigelände aus, in denen alle sicherheitsrelevanten Infrastrukturen des Krankenhauses von der Sauerstoffversorgung der Intensivbetten bis zur Glasfaserverkabelung der Datenverarbeitung frei zugänglich waren. Der Einsatz einer kräftigen Schere hätte genügt, um das Krankenhaus vollständig außer Funktion zu setzen und unerkannt zu entkommen. Dieser katastrophale Mangel wurde wegen Gefahr im Verzug sofort dem Krankenhaus mitgeteilt, welches sofortige Abhilfe versprach. Dies geschah dann doch mit Verzögerung, nachhaltigere Maßnahmen wurden in der Stellungnahme zum Prüfbericht versprochen. Einige Monate später wurde unangekündigt nachgeprüft: Die zunächst verschlossene Tür war wieder geöffnet, ein Stein hinderte sie am Zufallen, der Spaziergang konnte mit dem staunenden Datenschutzbeauftragten des Konzerns wiederholt werden. Da die Klinik mit der Privatisierung wie ein Privatbetrieb zu behandeln war und wir als Aufsichtsbehörde handelten, wurde zum ersten Mal vom Instrument der Anordnung technisch-organisatorischer Maßnahmen Gebrauch gemacht, das der Aufsichtsbehörde für den Datenschutz für solche Fälle im Datenschutz an die Hand gegeben worden ist.

2001

Der 11. September – auch ein Datenschutzdesaster

Der 11. September 2001 hinterließ weltweit tiefe Spuren bei der Verarbeitung personenbezogener Daten. In den USA war offenbar geworden, dass trotz vielfältiger Datensammlungen durch Abhören der internationalen Telekommunikation Terrorstraftaten dieser Größenordnung nicht verhindert werden konnten. Die sofortige Reaktion war, die Erhebung und Zusammenführung personenbezogener Daten aller Bevölkerungskreise zu intensivieren. Besonders betroffen waren Personen, die in oder durch die USA reisten. Die Übermittlung von Flugpassagierdaten einschließlich deren Essgewohnheiten und Behinderungen an die amerikanischen Einreisebehörden ist ein Thema, das nicht nur die Gemüter der Beteiligten, sondern auch das Europäische Parlament und den Europäischen Gerichtshof nach wie vor beschäftigen. „Biometrische Daten“ werden künftig in allen Reisedokumenten enthalten sein. Eine derartige „Volksdaktyloskopie“ war anfangs des 20. Jahrhunderts selbst in Kaiserzeiten als Verstoß gegen das Rechtsstaatsprinzip betrachtet worden.

Unmittelbare Folge der veränderten Sicherheitslage war, dass in Berlin wie auch in allen anderen Bundesländern die Rasterfahndung als Fahndungsmittel wiederentdeckt wurde. Ziel war es, „Schläfer“ aufzuspüren, d. h. Personen, die sich im terroristischen Umfeld befinden und möglicherweise Anschläge vorbereiten könnten. Zu diesem Zweck wurde ein Profil mit Merkmalen erstellt, die mögliche Schläfer haben könnten. Für die Erstellung dieses Täterprofils dienten die Eigenschaften der Attentäter des 11. September 2001 als Vorlage: u. a. männlich, Student, islamische Religionszugehörigkeit, ohne Familie. Zur Datenübermittlung zum Zwecke der Rasterung verpflichtet wurden zahlreiche Stellen, öffentliche wie private, des Landes Berlin.

Es brauchte einige Versuche, bis eine korrekte richterliche Anordnung für die Rasterfahndung vorlag. Andererseits zeigte sich, dass die Berliner Verwaltung darum bemüht war, die Kreise bei der Rasterung möglichst durch klare Ausschlüsse eng einzugrenzen. Dies ist ihr aus unserer Sicht auch gelungen. Auf diese Weise konnte die Zahl der erhobenen Daten von 58.063 Datensätzen auf am Ende 114 Personen, zu denen noch nachermittelt wurde, verringert werden.

Unsere Aufgabe bestand darin, bei den an der Rasterfahndung angefragten Stellen zu prüfen, ob sie die Daten zulässigerweise übermitteln durften. Die Fehler bei der Datenerhebung durch die Polizei haben wir geholfen zu beheben, so dass am Ende die Datenerhebung auf eine datenschutzrechtlich richtig formulierte Datenabfrage gestützt werden konnte.

Die Erfahrungen aller Beteiligten haben dazu geführt, dass die Rechtsgrundlage im ASOG noch einmal datenschutzrechtlich nachgebessert wurde.

2002

Unternehmensregelungen für den internationalen Datentransfer

Weltweit tätige Konzerne dürfen personenbezogene Daten in ihre Niederlassungen außerhalb der EU nur dann übermitteln, wenn beim datenimportierenden Unternehmen für ausreichende Datenschutzgarantien gesorgt ist. Nach dem Bundesdatenschutzgesetz von 2001 können sich diese Garantien „insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen“ ergeben.

Als weltweit erster Konzern hat die DaimlerChrysler AG eine derartige Unternehmensregelung für Kundendaten einerseits und für Mitarbeiterdaten andererseits auf den Weg gebracht. Nachdem sich die deutschen Aufsichtsbehörden unter unserem Vorsitz inhaltlich mit den Unternehmensregelungen befasst hatten, erteilten wir auf dieser Grundlage zwei Genehmigungen für Datenübermittlungen von Berliner Konzerntöchtern in die USA. Inzwischen wurden weitere Unternehmensregelungen in Deutschland verabschiedet (General Electric, Deutsche Telekom, ein Muster für die Versicherungswirtschaft) und auf ihrer Grundlage Genehmigungen für Datenübermittlungen in Drittländer erteilt (z. B. für Niederlassungen des US-Konzerns General Electric). Entsprechend dem Bedürfnis der Wirtschaft und der Aufsichtsbehörden in Europa ist 2004 unter unserem Vorsitz ein Verfahren zur europaweiten Koordinierung der Anerkennung von Unternehmensregelungen entwickelt worden.

Erste DNA-Reihenuntersuchung in Berlin

Im Juli 2002 wurde in der Babyklappe eines Berliner Krankenhauses ein Kleinkind abgelegt, das durch viele Messerstiche getötet worden war. Offensichtlich hatte die Person, die das tote Baby dorthin brachte, Ortskenntnisse. Die Polizei hat deshalb in Absprache mit der Staatsanwaltschaft – nachdem alle anderen Spuren mit hohem Aufwand verfolgt worden waren – die auf dem Krankenhausgelände beschäftigten Frauen um die Abgabe einer Speichelprobe gebeten, um einen Vergleich der DNA mit Tatspuren vorzunehmen.

Es war die erste große DNA-Reihenuntersuchung, die in Berlin durchgeführt wurde. Sie wurde auf die Einwilligung der Betroffenen gestützt. Zuvor hat die Polizei umfangreiche Aufklärungsarbeiten im Rahmen einer Personalversammlung geleistet, bei der die Hintergründe für das Vorhaben ausführlich erläutert wurden. Darüber hinaus befand sich ein Polizeimitarbeiter ständig im Krankenhaus, der den Kontakt zu den Beschäftigten hielt und insbesondere für Informationsgespräche zur Verfügung stand.

Die Datenschutzbeauftragten des Bundes und der Länder vertreten die Auffassung, dass die Einwilligung zur Entnahme, Analyse und Speicherung molekulargenetischen Körpermaterials keine Grundlage für einen derartigen Eingriff sein kann; eine wirksame Einwilligung setzt voraus, dass sie frei von jeglichen – auch psychischen – Zwängen freiwillig erfolgt. Da die Betroffenen annehmen können, dass eine nicht erteilte Einwilligung Auswirkungen auf ihr Ansehen im sozialen Umfeld haben kann, sie mit weiteren Besuchen der Polizei vor den Augen der

Nachbarschaft oder Ermittlungen beim Arbeitgeber rechnen müssen, und davon auszugehen ist, dass bei einem erfolglosen Verlauf des Gentests die Polizei ihre Ermittlungen auf diejenigen Personen konzentrieren wird, die eine Teilnahme verweigert haben, kann von einer Freiwilligkeit nicht mehr die Rede sein. Allerdings haben Gerichte in Berlin entschieden, dass bei Vorliegen einer Einwilligung des Betroffenen eine richterliche Anordnung der Maßnahme nicht mehr ergehen könne.

Es ist rechtsstaatlich höchst bedenklich, dass bei molekulargenetischen Reihenuntersuchungen die Beweislast umgekehrt und die Unschuldsvermutung durchbrochen werden. Die Aufforderung an unverdächtige Personen, sich selbst zu entlasten, darf nicht zu einem Standardfall der Strafermittlungen werden. Die kriminaltechnischen Reihentests dürfen nur bei herausragenden Fällen durchgeführt werden. Ihre Legitimation erhalten sie nur aufgrund des öffentlichen Interesses an der Aufklärung der Straftat – und nicht etwa aufgrund eines Interesses der Nichttäter an dem Nachweis, als Spurenverursacher ausgeschlossen zu werden. Aus diesem Grund wäre es sachgerechter, wenn die Tests nicht auf die Einwilligung, sondern auf die Entscheidung eines Richters gestützt würden. Im Juni 2004 hat die Polizei mitgeteilt, dass DNA-Reihenuntersuchungen künftig nur noch nach richterlicher Anordnung durchgeführt werden.

2003

Kundenbetreuung mit Getränkewunsch

Um Bankkunden in Vermögensangelegenheiten beraten zu können, benötigen Bankmitarbeiter verschiedenste Informationen über ihre Kunden, wie Vermögensstand, Anlagehorizont oder Risikobereitschaft. Der in Bankerkreisen häufig benutzte Slogan „Know your customer“ wurde von einer Bank etwas zu wörtlich genommen. Zur Verbesserung des persönlichen Kontaktes konnten die Berater Ess- und Trinkgewohnheiten ihrer Kunden (Kaffee, Tee oder eventuell schon am Morgen Alkohol) festhalten. Auch bei der Frage, wie der Berater am besten das Gespräch einleitet, sollte nichts dem Zufall überlassen bleiben. Deshalb sollte der

Berater auch mögliche Themen festhalten, wie Hobbys des Kunden (Golf, Fußball), Probleme im Beruf oder in der Beziehung, ja selbst gesundheitliche Probleme des Kunden hätte der Anlageberater festhalten können, sofern diese für die Gesprächseinleitung hilfreich erschienen. Außerdem sollten die Mitarbeiter Daten über alle Personen aufnehmen, die zum Kundenhaushalt gehören (Familienverbund). Dies sollte unabhängig davon geschehen, ob die Angehörigen selbst ein Konto bei der Bank hatten oder es für die Speicherung nachvollziehbare Gründe (gemeinsame Zinsabschlagsteuer) gab.

Auf unsere Empfehlung hin hat die Bank das Kundenbetreuungsprogramm „entschärft". Dies dürfte auch die Kundenzufriedenheit erhöht haben: Welcher Kunde möchte schon ständig von jemandem auf sein Hobby angesprochen werden, der daran möglicherweise gar kein Interesse hat. Auch die Ehepartner der Bankkunden dürften wenig begeistert davon sein, von einer Bank, bei der man nicht Kunde ist, als Anhängsel des Ehegatten geführt und beworben zu werden.

Controlling in der Berliner Verwaltung

Wenn die Berliner Verwaltung Fragen beantworten will, die noch gar nicht gestellt wurden, dann richtet sie ein „ziel- und wirkungsorientiertes Controlling" ein. So wurden wir von der Senatsverwaltung für Finanzen damit beschäftigt, einem von ihr beauftragten Software- und Beratungsunternehmen die Grundzüge des Datenschutzrechts im Wege des „learning by doing" beizubringen, als ein solches Controlling bei den Transferleistungen im Sozialhilfe-, Jugendhilfe- und Wohngeldbereich entwickelt und eingeführt werden sollte.

Warum soll denn der Finanzsenator sich personenbezogene Sozialdaten der Bezirke nicht liefern lassen, wenn er später einmal Auswertungen machen möchte, die ihm Fragen zur Effizienz der sozialen Angebote beantworten könnten? Warum soll dem Sozialamtsmitarbeiter nicht vom Computer des Finanzamtes gesagt werden können, dass bei dem vor ihm sitzenden Hilfeempfänger alle Müh vergebens ist, ihn in den Arbeitsmarkt einzugliedern? Warum soll denn die mühsam ausgehandelte Pseudonymisierung der Controllingdaten nicht wieder rückgängig gemacht werden können, wenn vielleicht ein Bundesgesetz kommt, welches sie nicht wie derzeit ausdrücklich verlangt? Warum muss das so schöne Auswertungssystem durch die Beseitigung des Personenbezugs abgespeckt werden, nur weil Rechtsgrundlagen fehlen und wohl auch nicht geschaffen werden? Die datenschutzrechtliche Begleitung der Vorabkontrolle war ein mühseliges Geschäft, denn zu jeder ausgehandelten Verbesserung des Datenschutzes kam der

Versuch, ihn wieder zu relativieren. Eine Springprozession: Zwei Schritt vor, einen zurück – am Ende wurde aber das Ziel erreicht.

Das Hausrecht reicht einen Meter weit

15 Jahre nach unserer ersten Überprüfung der Videoüberwachung in einer Bank sind Videokameras nahezu allgegenwärtig. Fassaden von Geschäfts- und Behördengebäuden zieren ganze Batterien dieser Geräte. Ein großes Kaufhaus im Zentrum Berlins hatten sich Bürgerrechtler auserkoren, die Zulässigkeit der Überwachung überprüfen zu lassen. Sie monierten insbesondere, dass mit den Kameras der Gehweg vor dem Kaufhaus erfasst würde und man den entsprechenden Straßenabschnitt nicht unbeobachtet passieren könne. Gleichzeitig haben wir eine Überprüfung vorgenommen.

Zunächst mussten wir feststellen, dass die nunmehr im Bundesdatenschutzgesetz vorgeschriebenen Hinweispflichten nicht in hinreichendem Maße realisiert waren – ein Mangel, der sehr häufig festzustellen ist. Die Videoüberwachung im Inneren entsprach den Vorschriften, nicht aber die Kameras im Außenbereich. In der Tat waren die Kameras in einer Weise angebracht und eingestellt, dass sowohl die Gehwege als auch wesentliche Teile der Fahrstraße im Blickwinkel lagen. Wir vertraten die Auffassung, dass allenfalls ein Streifen von einem Meter erforderlich ist, um die befürchteten Straftaten wie Einbruchsversuche oder Schmierereien zu verhindern. Dies muss auch dann gelten, wenn eine größere Fläche zwar zum Privatgrundstück gehört, aber von der Öffentlichkeit genutzt werden kann.

Im Dezember 1993 bestätigte das Amtsgericht Berlin unsere Auffassung. Die Kameras wurden neu justiert.

2004

Nach 25 Jahren: Das Mittelalter kehrt zurück

Die Presse kündigte es an: In Berlin sollte die Parkkralle von der öffentlichen Verwaltung bei der Vollstreckung von Schulden eingesetzt werden. Wie zuvor schon

in anderen Bundesländern getestet, testete auch das Land Berlin 2003 ein halbes Jahr lang den Einsatz einer Parkkralle zum Eintreiben säumiger Kraftfahrzeugsteuern. Die Vollstreckungsbeamten führten bei säumigen Steuerschulden (hier: Kfz-Steuerschulden) das Vollstreckungsverfahren durch und wiesen nach Anbringen des Pfandsiegels in einem Schreiben darauf hin, dass im Falle der Nichtbegleichung der Steuerschuld in den nächsten drei Tagen eine Parkkralle an das Auto angebracht werden wird, so dass der Fahrzeughalter oder Steuerschuldner es nicht mehr fortbewegen kann. Mit dieser Androhung wurde Druck auf die Betroffenen ausgeübt, die Steuerschuld zu begleichen, denn ansonsten könnten sie ihr Fahrzeug nicht mehr nutzen.

Bei der Parkkralle handelt es sich um eine nicht zu übersehende grellgelbe Wegfahrsperre, die jedem zeigt: Dieses Auto gehört einem Steuerschuldner. Ein Sprecher der Finanzverwaltung selbst hatte die Parkkralle gegenüber der Presse als Folterinstrument bezeichnet. Aus unserer Sicht stellt die Parkkralle die moderne Form des Prangers dar, da sie gut sichtbar für alle auf die Steuerschuld des Kfz-Halters hinweist. In der Abgabenordnung ist der Einsatz der Parkkralle nicht vorgesehen. Ihr Einsatz soll im Vollstreckungsverfahren vielmehr zusätzlichen Druck auf den Steuerschuldner ausüben. Im Gegensatz zum Pfandsiegel, dessen Einsatz in der Abgabenordnung gesetzlich geregelt ist, weist die gelbe Parkkralle schon von weitem auf die nicht bezahlte Steuerschuld hin. Und zumindest Nachbarn und Freunde dürften das Fahrzeug des Steuerschuldners wiedererkennen.

Im April 2004 erging die Anweisung der Finanzverwaltung, die Parkkralle nunmehr regelmäßig einzusetzen – natürlich ohne uns davon zu benachrichtigen.

Uns liegt eine Eingabe vor, dass der Einsatz der Parkkralle bereits bei einer Steuerschuld von 80 Euro als mögliches Vollstreckungsmittel angekündigt wurde, und dies obwohl im Vollstreckungsverfahren der Grundsatz der Verhältnismäßigkeit in besonderem Maße zu beachten ist und ein Fahrzeug mit hohem Zeitwert bei einer niedrigen Schuldsumme nicht verwertet werden dürfte.

Der Fantasie zur Eintreibung von Schulden durch den Staat sind offenbar keine Grenzen gesetzt. Angestrebt wird jetzt auch der Einsatz der Parkkralle an Fahrzeugen von Unterhaltsschuldnern.

Chronologie des Datenschutzes in Berlin

Vorgeschichte

15. Dezember 1890	Die Rechtsanwälte Samuel D. Warren und Louis D. Brandeis (später berühmter liberaler Bundesrichter am Supreme Court) veröffentlichen im Harvard Law Review einen bahnbrechenden Aufsatz zum Thema „The Right to Privacy“
1964	Der US-Kongress lehnt die Einführung einer Bundesdatenbank, in der alle US-Bürgerinnen und -Bürger mit Computern erfasst werden sollten, endgültig ab, da ein solcher Plan mit dem „Right to Privacy“ nicht vereinbar sei; ein Gesetz zur Regelung des Computereinsatzes wird gefordert
1969	Der deutsche Begriff „Datenschutz“ wird in Anlehnung an das Wort „Maschinenschutzgesetz“ geprägt; es findet in alle Weltsprachen Eingang (data protection; protection des données; zaschtschyta danych)
7. Oktober 1970	Als erstes Datenschutzgesetz der Welt wird das Hessische Datenschutzgesetz verabschiedet
31. Dezember 1974	Nach jahrelangen Diskussionen verabschiedet der 93. Kongress der USA den Privacy Act für die Bundesregierung; für den privaten Bereich gibt es bis heute kein umfassendes Datenschutzgesetz
27. Januar 1977	Das erste deutsche Bundesdatenschutzgesetz wird ausgefertigt

Datenschutz in Berlin

12. Juli 1978	Erstes Berliner Datenschutzgesetz
27. September 1979	Das Abgeordnetenhaus wählt Dr. Hans-Joachim Kerkau zum ersten Berliner Datenschutzbeauftragten
1. November 1979	Amtsantritt von Herrn Dr. Kerkau, Einrichtung der Dienststelle des Berliner Datenschutzbeauftragten im Europacenter
29. Mai 1980	Mit dem Bildschirmtext-Erprobungsgesetz wird in Berlin weltweit erstmals ein Gesetz geschaffen, das den Datenschutz bei den Neuen Medien regelt; die dort und im Bildschirmtext-Staatsvertrag vom 18. März 1983 enthaltenen Bestimmung dienen seither als Vorlage für alle Regelungen zum Datenschutz in der Telekommunikation
September 1983	Zum ersten Mal trifft sich die Internationale Arbeitsgruppe Datenschutz bei der Telekommunikation (damals noch: bei Neuen Medien) anlässlich der Internationalen Funkausstellung unter Vorsitz des Berliner Datenschutzbeauftragten; diese Arbeitsgruppe prägt seit Jahren die internationalen Aktivitäten auf diesem Gebiet im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten
Dezember 1983	Umzug der Dienststelle in die Hildegardstraße 28

Europacenter

Hildegardstraße 28

15. Dezember 1983	Das Bundesverfassungsgericht erklärt das Vorhaben einer Volkszählung 1983 für verfassungswidrig und stellt dabei Grundsätze für den Datenschutz auf, die eine Novellierung aller Datenschutzgesetze erforderlich machen
17. Juli 1984	Das Kabelpilotprojektgesetz setzt die Reihe datenschutzrechtlicher Regelungen bei der Telekommunikation für das Kabelfernsehen fort
30. August 1989	Internationale Datenschutzkonferenz in Berlin: Die Europäischen Datenschutzbeauftragten fordern energisch Aktivitäten der Europäischen Kommission auf dem Gebiet des Datenschutzes
16. November 1989	Dr. Hansjürgen Garstka wird zum Berliner Datenschutzbeauftragten gewählt
17. Dezember 1990	Das neue Berliner Datenschutzgesetz verwirklicht den Verfassungsgrundsatz der informationellen Selbstbestimmung in vorbildlicher Weise
20. Dezember 1990	Das ebenfalls novellierte Bundesdatenschutzgesetz lässt viele Wünsche offen
14. April 1992	Das Allgemeine Sicherheits- und Ordnungsgesetz wird überarbeitet; es enthält zwar nunmehr im Gegensatz zur vorherigen Fassung eine Reihe von Rechtsgrundlagen zur Verarbeitung personenbezogener Daten, schränkt aber den Datenschutz gegenüber dem allgemeinen Datenschutzgesetz erheblich ein
20. November 1992	Der Berliner Landesbeauftragte zur Aufarbeitung der Unterlagen des Staatssicherheitsdienstes der ehemaligen Deuschen Demokratischen Republik im Land Berlin wird im Geschäftsbereich des Berliner Datenschutzbeauftragten eingerichtet
Juni 1993	Umzug der Dienststelle in die Pallasstraße 25


Pallasstraße 25

3. Juli 1995	Änderung des Berliner Datenschutzgesetzes: Der Berliner Datenschutzbeauftragte übernimmt die Aufgabe der Aufsichtsbehörde für den privaten Bereich
24. Oktober 1995	Die Europäische Datenschutzrichtlinie tritt in Kraft; obwohl die dreijährige Umsetzungsfrist seit über einem Jahr verstrichen ist, verfügen bisher weder der Bund noch das Land über ein angepasstes Datenschutzgesetz
23. November 1995	Die neue Berliner Verfassung wird um das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Art. 33), sowie die Funktion des Berliner Datenschutzbeauftragten (Art. 47) ergänzt
30. Oktober 1999	Das Berliner Informationsfreiheitsgesetz tritt in Kraft. Es gewährt – bei Berücksichtigung des Datenschutzes – jedem Menschen das Recht auf Einsicht in die Unterlagen der Berliner Behörden; der Berliner Datenschutzbeauftragte übernimmt das Amt des Berliner Beauftragten für den Datenschutz und das Recht auf Akteneinsicht (später: Informationsfreiheit)
23. Mai 2001	Mit fast dreijähriger Verspätung tritt das neue Bundesdatenschutzgesetz in Kraft
12. Juli 2001	Auch das Berliner Datenschutzgesetz wird novelliert
Juni 2003	Umzug der Dienststelle An die Urania 4 – 10

An der Urania 4 – 10

Ein Aufkleber und seine parlamentarische Behandlung

Kleine Anfrage Nr. 33
der Abgeordneten Gabriele Rost (CDU)
über „Schnüffeln verboten“

Ich frage den Senat:

1. Trifft es zu, daß die Herstellung und Verteilung der Aufkleber „Schnüffeln verboten“ nicht etwa im Rahmen der Suchtpräventionsmaßnahmen von der Senatsverwaltung für Gesundheit, sondern vom Datenschutzbeauftragten veranlaßt wurde?

2. Welche Kosten sind durch diese Aktion entstanden?

3. Wo sollen aus der Sicht des Datenschutzbeauftragten diese Aufkleber angebracht werden (Wohnungstür, Küche, Toilette?), und welche praktische Wirkung sollen sie entfalten?

4. Ist der Senat der Auffassung, daß diese Aktion das Miteinander der Bürger untereinander und der Verwaltung gegenüber verbessern kann oder nicht viel eher geeignet ist, Mißtrauen zu säen?

Berlin, den 21. Januar 1991

Antwort auf die Kleine Anfrage Nr. 33

Im Namen des Senats von Berlin
beantworten wir Ihre Kleine Anfrage wie folgt:

Der Berliner Datenschutzbeauftragte ist eine oberste Landesbehörde. Er untersteht keiner Fachaufsicht. Nach dem Berliner Datenschutzgesetz (§ 12 Abs. 2) übt der Präsident des Abgeordnetenhauses lediglich die Dienstaufsicht über ihn aus. Daher wird nachstehend die uns vom Berliner Datenschutzbeauftragten übermittelte Antwort auf die Fragen 1 bis 3 wörtlich wiedergegeben.

Zu 1. bis 3.:
Aufkleber sind ein modernes Informationsmittel, um breite Bevölkerungsschichten auf dringliche Probleme aufmerksam zu machen. Dabei ist das Problem auf möglichst griffige Weise darzustellen. Gerade im östlichen Teil Berlins, wo Informationen über den Datenschutz und die Funktion des Datenschutzbeauftragten besonders dringlich sind, ist der gewählte Slogan „Schnüffeln verboten“ als treffende Kurzformel für die Wahrung der informationellen Selbstbestimmung mit großem Beifall aufgenommen worden.

Mißverständnisse sind uns nicht bekannt geworden; sollte jemand den Aufkleber als Warnung vor Drogenmissbrauch in der Form des „Schnüffelns“ auffassen, ist dies ein willkommener Nebeneffekt.

Der Datenschutz hat auch im Alltag große Bedeutung; die Anbringung an den vorgeschlagenen Stellen würde dies in besonderem Maße zum Ausdruck bringen.

Die Aufkleber haben 10.830,- DM gekostet.

Zu 4.:
Der Senat teilt die in der Frage enthaltene Befürchtung nicht, der Aufkleber könne geeignet sein, Mißtrauen zu säen.

Berlin, den 18. Februar 1991

Prof. Dr. Heckelmann
Senator für Inneres

Eingegangen am 25. Februar 1991

Zum Schluss: ein Silbenrätsel

Aus den folgenden Silben sind 17 Wörter zusammenzusetzen, deren erste und letzte Buchstaben – jeweils von oben nach unten – gelesen die Wurzel beschreibt, die den Datenschutz trägt (ü = ue). Es gilt die neue Rechtschreibung.

be – ben – ben – brauch – com – cke – da – da – dis – e – e – ein – ein – er – for – ga – ge – he – in – job – ka – klau – kre – kro – lass – lei – lek – lü – ma – ma – mi – miss – na – ne – ner – nig – on – ons – pu – rät – rech – rei – san – sicht – so – sus – ta – tät – te – ten – ten – ter – ter – ti – ti – tri – un – war – zen – zi

1. Alltägliches Kavaliersdelikt, damit leider immer währende Existenzberechtigung der Datenschützer
2. Dies zu bewirken, wirft man den Datenschützern vor. Der Mut dazu würde manche Entscheidung beschleunigen
3. Aufstehen – auch: Das Verschaffen von Daten
4. Böse Zungen behaupten, dies wäre die Hauptaktivität bei Internet-Surfen, beim Ski- und beim Bahnfahren
5. Ohne dies ist dauernd
6. Dosenware, die ein Computer braucht – und nicht nur er
7. Konsequente Form des Datendiebstahls
8. Sie schützt der Datenschutz nicht!
9. Legendäres Gerät zur Transportkontrolle
10. Datenschutz gesprächsweise
11. Erstkontaktstelle zur klassischen Datenverarbeitungsanlage
12. Musikalischer Elektroniker – später auch Golf-Bruder
13. Kleinste staatliche Neugierde – regelmäßiges Highlight für den Statistik-Referenten
14. Akzeptieren eigener Schwächen oder Alternative zur Auskunft
15. Für viele Datenschützer ist dies der Datenschutz
16. Orientalische und frühere Vorgängerin von Sozial-BASIS
17. Anglisierter Lockruf für ein männliches Geflügel

Lösung:

1. **D**ATENMISSBRAUC**H**
2. **I**NFORMATIONSLÜCK**E**
3. **E**RHEBE**N**
4. **W**ARTERE**I**
5. **U**NTERLAS**S**
6. **E**LEKTRIZITÄ**T**
7. **R**ECHNERKLA**U**
8. **D**ATE**N**
9. **E**NIGM**A**
10. **D**ISKRETIO**N**
11. **E**INGABEGERÄ**T**
12. **S**ANTAN**A**
13. **M**IKROZENSU**S**
14. **E**INSICH**T**
15. **N**EBENJO**B**
16. **S**OLEIK**A**
17. **C**OMPUTE**R**

DIE WUERDE DES MENSCHEN IST UNANTASTBAR