Peter Schaar

Das Ende der Privatsphäre

Peter Schaar

Das Ende der Privatsphäre

Der Weg in die Überwachungsgesellschaft

C. Bertelsmann

Verlagsgruppe Random House FSC-DEU-0100
Das für dieses Buch verwendete FSC-zertifizierte
Papier *Munken Premium* liefert
Arctic Paper Munkedals AB, Schweden.

1. Auflage
© 2007 by C. Bertelsmann Verlag, München,
einem Unternehmen der Verlagsgruppe Random House GmbH
Umschlaggestaltung: R·M·E Roland Eschlbeck/Rosemarie Kreuzer
Satz: Uhl + Massopust, Aalen
Druck und Bindung: GGP Media GmbH, Pößneck
Printed in Germany
ISBN 978-3-570-00993-2

www.cbertelsmann.de

Inhalt

Vorwort 9

1 Die verlorene Privatsphäre 11
1.1 Privatsphäre und Öffentlichkeit 15
1.2 Erste Leitplanken auf dem Weg in die Informationsgesellschaft 19
1.3 Nichts zu verbergen? 22
1.4 Schatten der Vergangenheit 27

2 Technologie und Datenschutz 32
2.1 Ein Blick zurück 32
2.2 Die Internetrevolution hat bereits stattgefunden 38
Angriffe aus dem Netz 40
Digitale Spuren 42
Das Netz vergisst nichts 47
2.3 Ubiquitous Computing – allgegenwärtige Überwachung? 49
Der Fluch permanenter Erreichbarkeit 50
Vernetzter Alltag 51
Funkchips – die heimliche Versuchung 53
2.4 Peilsender in der Jackentasche 56
2.5 Überall im Bild: Videoüberwachung 59
Revolution der Videotechnik 63

Vom Mautsystem zum Fahndungsinstrument? 66
Projekt Fotofahndung 68
2.6 Gesundheit aus dem Netz? 71
Mittels Gesundheitskarte zum gläsernen Patienten? 72
2.7 Der vermessene Mensch – biometrische Identifikationssysteme 75
Der Biometriepass 80
2.8 Ich weiß, wer du sein wirst – die Entschlüsselung des Genoms 83
Gentests – Objekte der Begierde 85
Genetischer Vaterschaftstest: Aus für »Kuckuckskinder«? 88
Eindeutig identifiziert: DNA-Identitätsfeststellung 90

3 Big Brother? Der Bürger im Blickfeld des Staates 94
3.1 Heute schon gezählt? Die Volkszählungsdebatte 99
Volkszählungsurteil des Bundesverfassungsgerichts 101
Datenschutz in der Verrechtlichungsfalle . . . 103
3.2 Großer Lauschangriff 106
3.3 Totalverlust Fernmeldegeheimnis? Überwachung der Telekommunikation 110
Nachrichtendienste hören mit 114
Vorratsspeicherung von Telekommunikationsdaten 116
3.4 Online-Durchsuchungen – »staatliches Hacking« 119

3.5 Datenschutz – Kollateralschaden im Krieg gegen den Terror? 124
Wer bleibt im Raster hängen? 128
»Otto-Kataloge« 131
Biometriepässe 133
Fluggastdaten für die USA 140
SWIFT – Finanztransaktionen im Visier der Terrorbekämpfung 144
Antiterrorlisten 147
3.6 Bürger unter Generalverdacht? 149
Polizei und Nachrichtendienste rücken zusammen 151
3.7 Die Kehrseite des Sozialstaats 157
Kostendruck gegen Datenschutz 160
ELENA – Datensammlung auf Vorrat? 162
3.8 Dürfen Finanzbehörden alles wissen? 164
Missverständnis Bankgeheimnis 165
Automatisierter Kontenabruf 166
3.9 eGovernment: Elektronische Verwaltung für mehr Bürgernähe? 169
Zusammenführung von Bürgerdaten 171
Identitätsmanagement 173
3.10 Der registrierte Ausländer 174

4 Ungehobene Schätze: Daten als Wirtschaftsfaktor 179
4.1 Geheimste Wünsche aufgedeckt – Werbung und Marketing 187
Widerspruchsrecht des Betroffenen 189
Spam und Telefonterror 192
4.2 Risikofaktor Kunde 195
Scoring 198

4.3 Gläserne Arbeitnehmer? 205
4.4 »Raubkopierer sind Verbrecher!« 211
Zugriff auf Internetdaten 215

5 Ist die Privatsphäre noch zu retten? 217
5.1 Datenschutz durch Technik 220
5.2 Modernisierung des Datenschutzrechts 226
Ethik der Informationsgesellschaft 230
5.3 Globaler Datenschutz 232

Dank 239

Anmerkungen 241
Register 245

Vorwort

Informationstechnische Systeme haben schleichend Besitz von unserem beruflichen und privaten Alltag ergriffen, und wir sind dabei, uns an immer umfassendere Kontrolle und Überwachung zu gewöhnen. Die Speicherung von Fingerabdrücken jedes Bundesbürgers in Ausweisdokumenten, die Antiterrordatei, eine immer lückenlosere Videoüberwachung, die vorsorgliche Speicherung der Daten jedes Telefonats und jedes Internetzugriffs, heimliche Online-Durchsuchungen privater PCs und die Einführung einer lebenslangen Steueridentifikationsnummer sind aktuelle Stichwörter der sich zuspitzenden Datenschutzdiskussion.

Das vorliegende Buch soll einen Beitrag zu dieser aktuellen Debatte leisten. Es richtet sich nicht nur an diejenigen, die sich ohnehin von Berufs wegen mit Fragen der Informationstechnik auseinandersetzen. Die Zukunft der Privatsphäre betrifft uns nämlich alle. Der Schutz der Privatsphäre ist viel zu wichtig, um ihn nur den »Fachleuten« – professionellen Datenschützern, Informatikern oder Juristen – zu überlassen.

Peter Schaar, 11. August 2007

1 Die verlorene Privatsphäre

Im November 2006 konfrontierte die Vertreterin einer Bürgerrechtsorganisation die Teilnehmer der Internationalen Datenschutzkonferenz in London mit einem drastischen Bild: »Ein Frosch, den man in einen Kessel sprudelnd heißen Wassers wirft, springt reflexartig sofort wieder hinaus. Setzt man den Frosch hingegen in einen Topf mit kaltem Wasser und erwärmt ihn allmählich, so bleibt er drin. Zunächst mag das sich erwärmende Wasser sogar recht angenehm sein. Wenn das Wasser weiter erhitzt wird, sind seine Kräfte erlahmt. Wenn es den Siedepunkt erreicht hat, ist er tot.« Anschließend stellte sie die Frage, ob es uns auf dem Weg in die Überwachungsgesellschaft nicht ähnlich ergeht wie jenem Frosch.

Gefahren drohen der Privatsphäre gleich von mehreren Seiten: Technologische Entwicklungen, wirtschaftliche Interessen, staatliche Kontrollen und auch die zunehmende Bereitschaft vieler Menschen, ihre eigene Privatsphäre nicht mehr ernst zu nehmen, gehen Hand in Hand. Im Folgenden sollen diese Entwicklungen näher betrachtet und Ansätze aufgezeigt werden, wie sich der Weg in eine allgegenwärtige Überwachungsgesellschaft abbremsen und vielleicht sogar umkehren ließe. Nur wenn sich die Gesellschaft und der Einzelne der Gefahren bewusst werden, wird die notwendige Umkehr erfolgen. Andernfalls müssen wir uns auf immer mehr Überwachung, Kontrolle und

Beeinflussung einstellen, und unsere rechtsstaatlichen Errungenschaften gehen Schritt für Schritt verloren.

Elektronische Systeme unterstützen uns bei allen möglichen Tätigkeiten. Sie bewahren uns vor eigenen Fehlern und sollen uns vor Bedrohungen aller Art schützen. Sie kommen auch dort zum Einsatz, wo wir sie nicht vermuteten, etwa beim Einkaufen und beim Autofahren: Wir können unseren »Datenschatten« nicht abschütteln.

Es kommt uns wie eine Geschichte aus grauer Vorzeit vor, als die meisten Computersysteme noch offline in großen Rechenzentren betrieben wurden und Dateneingabe und Auswertungen mit erheblichem Aufwand verbunden waren – Lochkarten mussten gestanzt, transportiert und eingelesen werden, die Ausgabe erfolgte in Form von perforiertem Endlospapier. Vergleicht man die heutige Situation mit dieser »Vorzeit«, die gerade einmal ein Vierteljahrhundert zurückliegt, wird die revolutionäre Veränderung deutlich: Miniaturisierte Computertechnik wird in alle möglichen Gegenstände des Alltags eingebaut. Die meisten Mikroprozessoren werden nicht etwa in Computern verwendet, sondern sie werkeln in Autos, Küchengeräten oder CD-Playern vor sich hin. Was liegt da näher, als diese Geräte miteinander zu vernetzen und so den Verbrauchern einen »Zusatznutzen« zu verschaffen, etwa indem – so ein gerne verwendetes Beispiel – der Kühlschrank online Nachschub bestellt, wenn die Butter zur Neige geht oder das Haltbarkeitsdatum der Milch überschritten wird? Doch dieser Zusatznutzen hat seinen Preis. Wir bezahlen ihn, ohne uns der Konsequenzen bewusst zu sein: Wo auch immer wir gehen und stehen, miteinander kommunizieren oder arbeiten, wird unser Verhalten nachvollziehbar (vgl. 2.3).

Überall wird unser Verhalten beobachtet, registriert und bewertet. Videokameras überwachen immer größere Bereiche des öffentlichen Raums und zeichnen auf, wo wir uns bewegen und mit wem wir Kontakt haben. Eine im Auftrag des britischen Datenschutzbeauftragten gefertigte Studie[1] kommt zu dem Ergebnis, dass in Großbritannien jeder Einzelne täglich von bis zu 300 Videokameras aufgenommen wird, Tendenz weiter steigend (vgl. 2.5).

Auch die Biometrie hat große Fortschritte gemacht. Verfahren zur automatischen Identifizierung von Personen anhand körperlicher Merkmale werden bereits in vielen Bereichen eingesetzt, etwa in den »ePässen«, bei Zugangskontrollsystemen im Betrieb oder beim Bezahlen an der Supermarktkasse (vgl. 2.7).

Wir sind heute per Handy überall erreichbar, und wir können mittels Satellitenortung metergenau feststellen, wo wir uns gerade aufhalten, wo sich unsere Kinder herumtreiben oder wo das Auto abgestellt ist. Auch Dritte können uns orten und die von uns zurückgelegten Wege nachvollziehen. Vielfältige neue Geschäftsmodelle, sogenannte »Location Based Services«, verwenden gerade diese Möglichkeiten, um uns etwa auf die nächste offene Tankstelle, ein italienisches Restaurant oder ein Modegeschäft in der Parallelstraße hinzuweisen (vgl. 2.4).

Die Verbindung verschiedener Überwachungstechnologien erschließt zusätzliche Einsatzfelder. So können digitale Videoaufnahmen mit den in Datenbanken gespeicherten biometrischen Referenzbildern abgeglichen werden, um die aufgenommenen Personen zu identifizieren. RFID-Funkchips (RFID = Radio Frequency Identification; damit werden Gegenstände und Menschen über Funk erfasst), die mit Kassensystemen und Kundenkarten gekoppelt

sind, erleichtern die Erzeugung von Kundenprofilen. Auch der Staat sammelt immer mehr Daten. Nachrichtendienstliche oder polizeiliche Ermittlungen können auch völlig Unschuldige betreffen. So muss man befürchten, als »Kontakt- oder Begleitperson« aufzufallen, die dann in einer entsprechenden Datei landet: sei es als Mitbewohner im Studentenwohnheim, in dem auch ein radikaler Islamist vermutet wird, als Arzt, der eine Zielperson medizinisch betreut, oder als Familienangehöriger eines Verdächtigen (vgl. 3.6).

Über die ganze Gesellschaft legt sich nach und nach ein unsichtbares Überwachungsnetz. Seine Existenz wird uns häufig erst dann bewusst, wenn wir selbst von negativen Folgen betroffen sind: Der wegen einer negativen Schufa-Auskunft verweigerte Kredit (vgl. 4.2), das von Unbekannten elektronisch leer geräumte Konto oder auch nur die von digitalem Werbemüll vollgestopfte Mailbox (vgl. 4.1) vermitteln eine Ahnung von den negativen Seiten der elektronischen Erfassungsgesellschaft. Jeder kann völlig zu Unrecht in Verdacht geraten, gegen Gesetze verstoßen zu haben, etwa bei der Inanspruchnahme des Internets. Wir müssen dann beweisen, dass wir keine urheberrechtlich geschützten Werke aus dem Netz geladen haben und dass die Anfrage in einer Suchmaschine oder der Abruf einer Webseite nicht etwa aus Sympathie für extremistische Bestrebungen, sondern aus wissenschaftlichem Interesse erfolgt ist.

Es ist nur noch eine Frage der Zeit, bis unsere elektronischen Persönlichkeitsprofile und digitalen Abbilder ein regelrechtes Eigenleben führen, wie es in elektronischen »Zweitwelten« im Internet à la »Second Life« schon spielerisch erprobt wird. Noch besteht die Chance, dass un-

sere Gesellschaft diesem digitalen »Frankenstein-Erlebnis« einen Riegel vorschiebt. Es ist höchste Zeit, dass wir aufwachen.

1.1 Privatsphäre und Öffentlichkeit

Die private und die öffentliche Sphäre sind seit Jahrhunderten untrennbar miteinander verbunden: Die Privatsphäre ist Raum des individuellen Rückzugs und zugleich unverzichtbare Voraussetzung einer freien Meinungsbildung. Totalitäre Systeme haben deshalb stets versucht, sowohl die öffentliche als auch die private Sphäre einer vollständigen Kontrolle zu unterwerfen. Ohne einen geschützten Raum, in dem man unbeobachtet und unzensiert über seine Erfahrungen und Einstellungen reflektiert und sich mit anderen austauscht, kann es auch keine freie Öffentlichkeit geben. Freie Rede, freie Information und freie Meinungsäußerung würden ohne ein tief verankertes Recht auf Privatheit verkümmern[2].

Die sich wandelnden Vorstellungen über die Beziehung zwischen öffentlicher und privater Sphäre lassen sich bis in die Antike zurückverfolgen. Bereits in den griechischen Stadtstaaten entwickelten sich zwei voneinander klar geschiedene Seinsordnungen heraus, eine private und eine öffentliche. Die private Ordnung des Hauses (»oikos«) bildete dabei den Gegenpart zur öffentlich-politischen Sphäre des Marktplatzes (»agora«). Bei den Römern setzte sich diese Zweiteilung der Lebenswelten fort, die sich bis in unsere Tage erhalten hat. Aus dem Lateinischen stammt auch der Begriff der Privatheit; ausgehend vom Verb »privare« (berauben), bezeichnete »privatus« den

Bürger, soweit er sich nicht politisch betätigte und der öffentlichen Beobachtung entzogen, »beraubt« war. Aus diesem Wortsinn heraus lässt sich herleiten, dass die private und die öffentliche Sphäre zwar zwei getrennte Welten repräsentierten, sich jedoch aufeinander bezogen. Zum Bürger wurde das Individuum erst dann, wenn es sich auch politisch, das heißt öffentlich betätigte. Das deutsche Wort »privat« wird seit dem 16. Jahrhundert verwendet und bezeichnet Sachverhalte bzw. Personen, die für sich stehen, also unabhängig sind.[3]

Die Privatsphäre in ihrer heutigen Bedeutung und ihr Gegenstück, die moderne Öffentlichkeit, sind ein Produkt der bürgerlichen Gesellschaft. In den meisten vorindustriellen Gesellschaften gab es keine Vorstellung von Individualität im heutigen Sinne. Vielmehr dominierten ererbte, rollenbezogene Zuordnungen. Mit dem Übergang zur bürgerlichen Gesellschaft verschwanden natürlich nicht die klassen- bzw. rollenspezifischen Unterschiede, aber ihre Ausdrucksformen änderten sich. Das von der Französischen Revolution 1789 proklamierte Gleichheitsideal war zugleich ein Abschied von der Vorstellung einer gottgegebenen, öffentlich inszenierten »ewigen« Rollenverteilung. Insbesondere beim Bürgertum wuchs der Wunsch, die individuellen Verhältnisse und Vorlieben der öffentlichen Wahrnehmung zu entziehen, vor allem um geschäftliche Entscheidungen ungestört von Einblicken Dritter vorzubereiten. Darin zeigt sich eine wesentliche Funktion von Privatheit: In einer von individuellen Entscheidungen geprägten Gesellschaft muss die Privatsphäre gegen Einblicke Dritter geschützt werden, damit das individuelle öffentliche Handeln überhaupt möglich ist.[4]

Der Presse kam bei der Herausbildung der modernen Öffentlichkeit entscheidende Bedeutung zu. Informationen wurden durch Zeitungen wesentlich schneller, weiter und weniger kontrollierbar verbreitet als durch mündliche Überlieferung oder über direkte Briefkontakte. Damit vergrößerte sich auch die Reichweite von Öffentlichkeit. Die Öffentlichkeit wurde sowohl sozial als auch geografisch entgrenzt, denn die Informationen standen einem immer breiteren Publikum zur Verfügung – über die lokalen oder regionalen Grenzen hinaus. Damit konnte der Einzelne die Verbreitung der auf ihn bezogenen Informationen nicht mehr kontrollieren.

Das autonome Individuum, das Ideal der bürgerlichen Gesellschaft, brauchte gerade angesichts der verbesserten Kommunikationsmittel einen privaten Raum, in dem es sich frei von Beobachtung bewegen und informieren, kommunizieren und Entscheidungen treffen konnte, ohne gegenüber der Öffentlichkeit rechenschaftspflichtig zu sein. Je »öffentlicher« die Öffentlichkeit wurde, je größer also der Radius der veröffentlichten Informationen wurde, desto dringender wurde der Schutz der Privatheit.

Seit Mitte des 20. Jahrhunderts haben die Veränderungen der Massenmedien das Verhältnis von privater und öffentlicher Sphäre in dramatischer Weise verschoben und die Grenze zwischen öffentlichem und privatem Verhalten immer undeutlicher werden lassen. Indem die Medien vorzugsweise über persönliche Angelegenheiten berichten, bewirken sie einen Verlust von Privatheit. Dies betrifft vor allem diejenigen, die ohnehin ein hohes Maß an öffentlicher Aufmerksamkeit genießen, also Prominente aus Politik, Showbusiness und Sport. Viele Vertreter aus diesen Bereichen nutzen die neuen Möglichkeiten

sogar für eigene Zwecke aus, etwa durch »Homestories« oder bei der öffentlichen Inszenierung privater Ereignisse wie Hochzeit, Schwangerschaft, Krankheit, Scheidung und Tod. Aber auch Nichtprominenten wird eine Bühne geboten, sei es in Talkshows, bei denen der Peinlichkeitsgrad der Teilnehmer das entscheidende Auswahlkriterium zu sein scheint, sei es im »Reality TV«, das sich bezeichnenderweise selbst mit dem Begriff »Big Brother« schmückt.

Die neuen Formen öffentlicher Darstellung lassen nicht nur die Privatsphäre der davon Betroffenen verschwinden. Vielmehr wird auch durch die gängige Berichterstattung über Privatangelegenheiten die durch die Medien stark geprägte Öffentlichkeit banalisiert und entpolitisiert. So gerät das private Verhalten von Politikern immer öfter ins Blickfeld der Öffentlichkeit und wird bisweilen detaillierter beobachtet und ausgebreitet als ihr öffentliches Handeln als Abgeordnete oder Minister. In den USA wurde eine von Präsident Clinton nominierte Generalstaatsanwältin deshalb nicht vom Kongress bestätigt, weil sie einige Jahre vorher eine illegale Einwanderin als Kindermädchen beschäftigt hatte. Derselbe US-Präsident entging nur knapp der Amtsenthebung aufgrund eines Techtelmechtels mit einer Praktikantin. In Schweden musste eine Ministerin zurücktreten, weil sie die Rundfunkgebühren nicht bezahlt hatte. In die gleiche Richtung weist, dass in Deutschland in manchen Medien über die Frisur der Bundeskanzlerin ausführlicher berichtet wird als über ihre Politik.

Ganz allgemein lässt sich feststellen, dass Privatangelegenheiten heute weitaus freizügiger öffentlich gemacht werden – bis hin zu intimen Details, deren Erörterung in

früheren Zeiten selbst im privaten Kreis weitgehend tabu war. Auch bei der Benutzung von Mobiltelefonen, Laptops und ähnlichen technischen Gerätschaften im öffentlichen Raum werden Privatangelegenheiten bedenkenlos offenbart. Private Homepages, Chatrooms, digitale Fotoalben und andere Internetangebote sind gerade deshalb erfolgreich, weil die Betroffenen möglichst freigebig über ihr Privatleben berichten und damit ohne jeden Zwang ihre Persönlichkeitsprofile einer weltweiten Öffentlichkeit gegenüber offenbaren.

Wir müssen – als Einzelne und als Gesellschaft – lernen, mit den neuen digitalen Dimensionen unseres Lebens umzugehen. Dazu gehört in erster Linie ein waches Bewusstsein dafür, was mit den preisgegebenen Informationen geschehen kann. Notwendig ist aber auch ein angemessener Schutz gegen Registrierung, Verfälschung und Manipulation. Dies ist eine wichtige, aber leider völlig vernachlässigte Aufgabe des Staates in der Informationsgesellschaft. Die Politik hat auf diesem Feld bisher sträflich versagt: Während staatliche Stellen – von der Polizei bis zur Finanzverwaltung – immer mehr über uns wissen wollen, bleiben die Bürger ohne angemessenen Schutz gegen Ausspionieren, Missbrauch, Manipulation und Verfälschung ihrer Daten.

1.2 Erste Leitplanken auf dem Weg in die Informationsgesellschaft

1890 veröffentlichten die amerikanischen Anwälte Samuel Warren und Louis D. Brandeis den bahnbrechenden Aufsatz »The Right to Privacy«.[5] Darin leiteten sie aus

den Rechtsgrundsätzen des Schutzes der Person und des Eigentums ein »Right to be left alone« ab, also das Recht eines jeden Menschen, von anderen in Ruhe gelassen zu werden. Bereits aus diesem Prinzip ergibt sich, dass der Bürger selbst über die Preisgabe der ihn betreffenden Informationen entscheiden soll. Das »Recht auf informationelle Selbstbestimmung«, dem das deutsche Bundesverfassungsgericht in seinem Volkszählungsurteil (vgl. 3.1) fast hundert Jahre später zum Durchbruch verhalf, hat hier seine Wurzeln.

Die Anfang der Sechzigerjahre von der Kennedy-Administration geplante Einrichtung einer nationalen Datenbank mit einer Vielzahl von Informationen über jeden US-Bürger führte zu einer ersten breiten Debatte über die Auswirkungen des Einsatzes von Computern auf die Privatsphäre. Dabei wurden die von der staatlichen Überwachung ausgehenden Gefahren ebenso kritisch bewertet wie die Risiken einer missbräuchlichen Datenverarbeitung durch Unternehmen. Der US-Kongress klammerte in dem 1974 verabschiedeten »Privacy Act« jedoch die Wirtschaft aus, weil er nicht in den Wettbewerb eingreifen wollte. In der Folge zeigten sich die Schwächen dieses beschränkten Ansatzes: Wenn Unternehmen sich ungestraft durch einen besonders aggressiven oder ausufernden Umgang mit personenbezogenen Daten einen wirtschaftlichen Vorteil verschaffen können, führt die Marktlogik nicht automatisch zu einem besseren Datenschutz. Dies bedeutet im Umkehrschluss jedoch nicht, dass jeder Versuch, einen effektiven Datenschutz auch über den Markt durchzusetzen, von vornherein zum Scheitern verurteilt ist. Allerdings müssen dafür Rahmenbedingungen gesetzt werden, die einen verantwortungsbewussten Umgang mit

personenbezogenen Daten wirtschaftlich belohnen (vgl. 5.2). Problematisch war auch die Entscheidung des US-Senats gegen eine unabhängige Datenschutzkontrolle.

Die Auseinandersetzung mit den Schwächen des US-Ansatzes trug dazu bei, dass Europa auch die von der US-Gesetzgebung ausgeklammerten Bereiche berücksichtigte. Bereits die Europaratskonvention von 1981[6] bezieht den nicht öffentlichen Sektor mit ein. Die Europäische Datenschutzrichtlinie von 1995[7] und die Datenschutzgesetze der EU-Mitgliedsstaaten machten eine unabhängige Datenschutzkontrolle für öffentliche Institutionen und für private Organisationen und Unternehmen verbindlich.

Der Begriff »Datenschutz« wurde erstmalig 1972 durch das hessische Datenschutzgesetz, das weltweit erste Datenschutzgesetz überhaupt, in das deutsche Rechtssystem eingeführt und 1977 in das Bundesdatenschutzgesetz übernommen. Der Begriff und seine direkten Übersetzungen (»data protection«, »protection des données« usw.) sind missverständlich, denn vielfach kommt es zur Verwechslung mit dem Begriff der Datensicherheit. Während es bei Letzterer darum geht, unzulässige Zugriffe auf Daten und ihre Verfälschung technisch zu unterbinden, soll der Datenschutz jedoch die Würde, Privatsphäre und Handlungsfreiheit der Individuen gewährleisten – ein wesentlich umfassenderer Anspruch.

Die noch heute gültigen Regelungsansätze mögen in den Achtzigerjahren angemessen gewesen sein; für die heutige Welt der allgegenwärtigen Datenverarbeitung (vgl. 2.3) reichen sie nicht mehr aus. Außerdem musste der Datenschutz seither vielfältige Rückschläge einstecken, vor allem im Hinblick auf immer weiter gehende Eingriffe in die Pri-

vatsphäre, die mit der Kriminalitätsbekämpfung begründet wurden (vgl. Kapitel 3).

1.3 Nichts zu verbergen?

Immer wieder wird mit dem populären Argument gegen den Datenschutz polemisiert, wer nichts zu verbergen habe, der brauche auch keinen Datenschutz. Immer wieder kann man allerdings feststellen, dass diejenigen, die gegen den Datenschutz anreden, ganz anderer Meinung sind, wenn es um sie selbst, wenn es um die eigenen Daten geht. Bereits der erste Bundesdatenschutzbeauftragte Hans Peter Bull hatte sich mit diesem Argument auseinanderzusetzen:

> »Wie dem auch sei – die Behauptung, man habe vor den Behörden oder den Mitmenschen nichts zu verheimlichen, widerspricht allen Erfahrungen des Alltagslebens. Da will doch jeder nur das über sich, seine Familie, seinen Beruf und seine Geschäfte verbreiten, was ihm vorteilhaft erscheint, und selbst derjenige, der sich gern selbst ironisiert oder aus öffentlicher Selbstkritik Befriedigung gewinnt, vermeidet es im Allgemeinen, sich ernsten Gefahren auszusetzen. Wer wird schon ohne Not bekennen, gegen ein Strafgesetz verstoßen zu haben? Wer wird durch unnötiges Offenbaren wirtschaftlicher Bedrängnis seinen Kredit gefährden? Und höchstens ein törichter Angeber wird durch unbedachtes Reden den Eindruck erwecken, nachrichtendienstliche Beziehungen zu unterhalten, sodass die Aufmerksamkeit der Sicherheitsbehörden auf ihn fällt.«[8]