Wie steht es um den Datenschutz? - Marc-Oliver Pahl Februar 2003

Der Artikel ist für das Informatik und Gesellschaft Seminar „Mathematik und Ethik“ von Dr. Gregor Nickel und Dr. Markus Wacker im Wintersemester 2002/ 2003 an der Universität Tübingen entstanden.

Inhaltsverzeichnis

Privatsphäre — ein menschliches Grundbedürfnis 3
Entwicklung der Datenerhebung 4
Automatisierte Datenverarbeitung — Computer 4
Datenerhebung in Deutschland 5
Das erste Datenschutzgesetz der Welt 7
Die europäische Union 10
Die USA 11
Datenschutz in Zeiten der Globalisierung 11
Fazit 15
Quellen 16

Abstract

Nach einem kurzen Abriss der Entwicklung der Datenerfassung von der Steintafel hin zum Computer wird die neuerliche Geschichte der Datenerhebung in Deutschland ab dem Hitler-Regime näher betrachtet. Der Fokus liegt dabei auf der Gesetzgebung, die sich seit 1974 mit dem Datenschutz befasst und schließlich 1995 zumindest teilweise in die EU-Datenschutzrichtlinie mündet. Anschließend wird kurz als Kontrast das amerikanische System der „Codes of Conduct“ beschrieben. Abschließend werden unter Berücksichtigung aktueller Entwicklungen eine Beurteilung der aktuellen Lage und ein Ausblick auf die Zukunft gegeben.

Wie steht es um den Datenschutz?

Informationsstand Februar 2003
Version vom Februar 2004

Privatsphäre — ein menschliches Grundbedürfnis

Jeder Mensch hat ein Privatleben, das nur ihn etwas angeht und bei dem er selbst entscheiden will, wen er daran teilhaben lässt. Dieses Grundbedürfnis findet seinen Niederschlag in den Mauern, die wir um uns aufbauen: Äußerlich beispielsweise im Zelt bzw. im Haus, das geschlossen werden kann und somit das „Außen“ vom „Innen“ trennt. Innerlich zum Beispiel darin, dass wir nicht jedem alles mitteilen, was uns gerade durch den Kopf geht —wir grenzen unseren privaten Bereich ab.

Dass in diese Schutzzone nicht eingedrungen wird, sonden sie im Gegenteil respektiert und geschützt werden muss, ist in den allermeisten Kulturkreisen selbstverständlich und hat daher auch seinen Niederschlag in der Menschenrechtscharta der Vereinten Nationen in Artikel zwölf gefunden (siehe rechts). Entsprechendes steht auch im Grundgesetz der Bundesrepublik Deutschland. Dessen Artikel eins und zwei gehen dabei noch deutlich über die Menschenrechtscharta hinaus, indem sie die freie Entfaltung der Persönlichkeit nur durch die Verfassung und die Persönlichkeitsrechte der anderen begrenzen (siehe dazu rechts).

Mit dem Übergang ins „Informationszeitalter“ scheint sich am Schutzbedürfnis der Menschen etwas zu ändern. Aktuelles Beispiel dafür ist die Fernsehserie BigBrother, die nun schon in der vierten Staffel läuft. Die Teilnehmer der Sendung tragen ihr komplettes Leben an die Öffentlichkeit und verzichten damit gänzlich auf Privatheit. Hauptanreiz dazu ist die Chance, 100 000 Euro zu gewinnen oder wenigstens durch die Serie „berühmt“ zu werden. Interessant ist, dass dies keine Randerscheinung der Gesellschaft zu sein scheint, sondern es im Gegenteil eine riesige Anzahl von Bewerbungen gibt und die Sendung einen großen Marktanteil hat. Es finden sich also Zuschauer und Kandidaten; der Wert der Privatsphäre scheint gering geworden und das Bedürfnis nach deren Schutz nicht mehr allzu groß zu sein.

Ein nicht so extremes und uns direkter betreffendes Beispiel sind Gewinnspiele oder „Gratis“-Dienstleistungen, deren eigentlicher Zweck es ist, Daten zu sammeln. Für die Gewinnchance auf ein Auto oder noch viel geringere Preise geben wir unsere Adresse, unser Alter und eventuell auch noch viel persönlichere Details preis. Die klassische Form solcher Datensammelspiele waren Gewinnpostkarten in Supermärkten. Die neuere, für den Anbieter deutlich preiswertere, und daher auch weiter verbreitete Form sind Fragebögen im Internet. Bereitwillig füllen wir zum Teil mehrere Seiten lange Fragebögen (GMX-Anmeldung) mit unseren Hobbys, Vorlieben, Ehedaten etc. aus. Bevor ich zur aktuellen Situation komme, will ich zunächst die historische Entwicklung bis heute beleuchten.

„Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Ruf ausgesetzt werden. Jeder Mensch hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Anschläge.“

UN-Menschenrechte Artikel 12

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“

Grundgesetz Artikel 1 Absatz 1

„Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“

Grundgesetz Artikel 2 Absatz 1

Entwicklung der Datenerhebung

Das älteste schriftlich festgehaltene Zahlensystem findet sich auf einer Tontafel aus der sumerischen Stadt Uruk im heutigen Irak. Die Tafel diente wohl der Verwaltung von Warenbeständen. Sie ist datiert auf 3300 vor Christus.

Als Merkmal für eine Hochkultur wird „Erfassung des gesellschaftlichen Wissens durch den Staat und die Erhebung von Tributen und Steuern, um den Staat zu finanzieren“[dietschi] angeführt —also Datenerhebung (siehe auch links). Brisanter als Daten über Waren ist Information über Menschen. Vor allem durch Erhebungen im Zusammenhang mit Steuern wurde solche Information angesammelt. Im römischen Stadtstaat (753-4. Jahrhundert vor Christus) musste sich jeder mündige Bürger alle fünf Jahre auf dem Marsfeld einfinden, um Auskünfte über seine Familien- und Vermögensverhältnisse zu machen: die professio censualis. Kaiser Augustus schreibt z.B. von solchen Zählungen unter seiner Herrschaft (um Christi Geburt) in seinen res gestae divini augusti.

Wie wir gesehen haben, gibt es schon sehr lange Datenerhebung und -speicherung vor allem durch den Staat. Volkszählungen als wohl größte gleichzeitige Erhebung von Daten gibt es auch heute noch. Bei der letzten amerikanischen Volkszählung 1990 wurden folgende Dinge erfragt: Name, Geschlecht, Geburt/ Tod, Kinder, Wohnort, Referenzverbände (Staat, Verein, Religionsgruppe etc.), Ausbildung, Beruf, Familienstand, Eltern, Lebensunterhalt (ökonomische Basis)[langPauli2002] —viele (private) Daten. Die größte Datensammlung ist für sich aber wertlos. Die Daten gewinnen ihren Wert erst durch ihre Auswertung in Bezug auf eine bestimmte Fragestellung, also zum Beispiel, indem wir die Anzahl der Berufstätigen bestimmen und so die Rentensteuer festlegen. Mit Steintafeln und Rechenschiebern war solch eine Auswertung beschwerlich und auch die teilweise noch heute im Einsatz befindliche Datenhaltung in Karteien (links) lässt eine schnelle Auswertung der Daten nur in Bezug auf die Sortierschlüssel, nach denen die Karten abgelegt sind, zu; in der Unibibliothek beispielsweise nach Titel, Autor und Jahr. Mit dem zunehmenden Bedarf an Auswertung von Daten entstand daher eine neue Maschine: der Computer.

Karteischrank

Automatisierte Datenverarbeitung — Computer

Die erste Datenauswertungsmaschine wurde 1890 von Hermann Hollerith, dem Leiter des für die Volkszählung zuständigen statistischen Bundesamtes in Washington erfunden. Nachdem seine 500 Sachbearbeiter für die Daten von 1880 sieben Jahre benötigt hatten, dauerte die Auswertung der Erhebung von 1890 mit nur 50 Mitarbeitern gerade einmal vier Wochen. Möglich geworden war dies durch die Verwendung von Lochkarten, die von Maschinen (siehe links) wesentlich schneller und genauer gelesen werden konnten als von Hand.

Hollerith-Maschine zum Auswerten der Lochkarten

Die riesigen Resourcen, die Ende des 19. Jahrhunderts noch benötigt wurden, um die Daten auszuwerten (sieben Jahre und 500 Mitarbeiter), verhinderten eine weitergehende Nutzung. Die Maschinen, die in der folgenden Zeit immer leistungsfähiger wurden, arbeiteten dagegen fast umsonst und sehr schnell. Jetzt war es erstmals möglich, große vorhandene Datenbestände flexibel auf viele Fragestellungen hin zu untersuchen. Erst der Computer hat also die Möglichkeit zu einer effizienten Datenauswertung geschaffen!

Datenerhebung in Deutschland

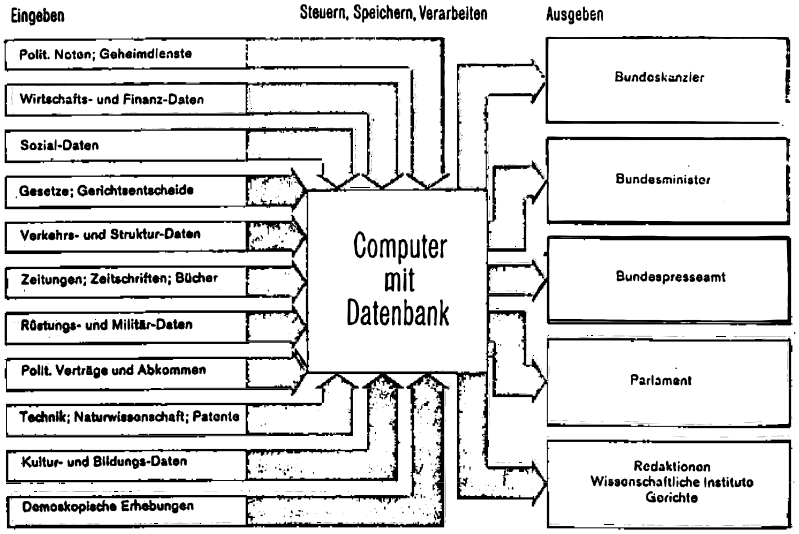
In Deutschland fanden die ersten Massendatenerhebungen 1933 unter Hitler noch auf Karteikarten statt. Sie waren wichtig, weil so die Wehrpflichtigen, die arbeitsfähige Bevölkerung, die Juden und andere für die Regierungsziele relevante Gruppen lokalisiert werden konnten. Um eine noch lückenlosere Erfassung der Bevölkerung zu bekommen wurden 1935 von Hand die Karteien der Arbeitsämter, die Arbeitsbuchkarteien und die Volksmeldekartei zusammengeführt, um mit den dadurch gewonnenen neuen Erkenntnissen noch effektiver Kriegsdienstverweigerer, Juden und andere für den Staat als Verbrecher geltende Personen aufzuspüren. Der Aufwand war beträchtlich und wäre unter normalen Umständen nicht bezahlbar gewesen. 1945 —nachdem man Hollerith-Maschinen erbeutet hatte— wurde begonnen, die Daten auf Lochkarten zu übertragen (siehe rechts). Mit dem Sieg der Alliierten über Hitler endete dieses Vorhaben dann.

Meldekarte im Dritten Reich

Das Dritte Reich zeigt besonders gut die Macht von Information und damit von Daten auf. Wer beispielsweise einmal als Jude im System erfasst war, hatte kaum noch Chancen, zu entkommen. Um die gefährliche Überwachung der Bürger durch den Staat (GeStaPo), wie sie unter Hitler stattfand, zu unterbinden, legten die Alliierten im Westen die Melderegister (Einwohnermeldeamt, Ausweiswesen) in die Hände der Länder. Im Osten wurde dagegen ein „Sicherheitsdienst“ —ab 1950 Ministerium für Staatssicherheit (Stasi)— aufgebaut, dessen Folgen für das Leben in der DDR uns spätestens seit der Wiedervereinigung bekannt sind.

Nach dem Krieg war der Datenschutz für die Bevölkerung in Anbetracht der Zerstörung und des Elends verständlicherweise kein so dringendes Anliegen. Aber auch in anderen Ländern interessierte man sich nicht dafür. Ende der sechziger Jahre gab es parallel in Deutschland und in den USA Pläne zum Anlegen eines zentralen Melderegisters. In beiden Ländern führte dies zu erbittertem Widerstand aus Bevölkerung und Presse, weshalb die Entwürfe fallengelassen wurden.

Das Diagramm auf der nächsten Seite zeigt sehr gut, für wie mächtig man die Datenverarbeitung mithilfe der neuen elektronischen Rechner hielt. Es war ein zentrales computerbasiertes Informationssystem geplant, in dem alle Daten, die überhaupt nur anfallen, gespeichert werden sollten. Wenn wir die Massen an Informationen betrachten, die heute auf uns einströmen, erscheint uns dieses Vorhaben als aussichtslos. Ich möchte aber zu bedenken geben, dass es 1968 weder Internet, noch Privatfernsehen in Deutschland gab. Sowohl demoskopische Erhebungen, wie unsere Volkszählungen, als auch Sozialdaten, Wirtschafts- und Finanzdaten, alle Verlagserzeugnisse, Kultur- und Bildungsdaten u.v.m. finden sich in der Grafik. Interessant ist auch, wem die Daten zur Verfügung stehen sollten.



Capital 9/ 1968 Seite 14: Vorhaben der Bundesregierung zu einer zentralen Datenerhebung [gehring et al. 2000]

Zur technischen Realisierung solch eines Ansatzes zur Speicherung aller Daten findet sich näheres im Zusammenhang mit Ted Nelsons Projekt Xanadu, das es seit 1965 gibt und im Artikel Ted Nelson, Dream Machines: new freedoms through computer screens - A minority Report. Computer Lib: You can and must understand computers now, Hugo's Book Service Chicago 1974.

Solch eine riesige Fülle von Informationen an einem zentralen Ort wäre eine unüberschaubare Macht und damit Gefahr für jeden Einzelnen gewesen: die Möglichkeit zur totalen Überwachung. Auch wenn Obiges nicht umgesetzt wurde, ist durch den damals einsetzenden Einzug des Computer in die Behörden das Datenaufkommen bis heute immer mehr angewachsen —wenn auch dezentral. Wie schon im Abschnitt „Automatische Datenverarbeitung - der Computer" angeführt, müssen Daten auf Papier von Hand sortiert und archiviert werden und sind nur mit größerem Aufwand wieder zugänglich. Die von da an entstehenden Daten im Computer sind dagegen vollautomatisch auswertbar und entstehen zum Teil sogar von selbst (z.B. Datum der Bearbeitung, Bearbeiter, letzter Besuch bei der Behörde). Die für den Datenschutz entstehende Gefahr war aber dadurch gering, dass die Daten nur dezentral in den entsprechenden Behörden vorlagen und auch die in unterschiedlichen Ämtern eingesetzten Softwareprodukte zumeist inkompatibel zueinander waren. Die neuerliche Verbreitung von Netzwerken, vor allem dem Internet, lässt das Wort dezentral aber bedeutungslos werden. Egal, wo die Daten liegen, können sie —bei entsprechender Zugangsberechtigung— überall sofort abgerufen werden. Der Weg hin zur Vernetzung der Datenbestände und deren Verknüpfung ist sogar erklärtes Ziel der Schröder-Regierung. Im Zuge der eGovernment-Initiative sollen bis 2005 „sämtliche Verwaltungsleistungen zusätzlich zu den bisherigen Wegen auch über das Internet vollständig [abwickelbar gemacht werden]" [eGovernment]. Das ist von Vorteil, weil an mehreren Stellen benötigte Daten nur einmal erhoben werden müssen. Damit ist zumindest technisch aber auch die Möglichkeit zu einer einfachen totalen Überwachung jeglicher Interaktion mit dem Staat geschaffen.

eGovernment-Initiative des Bundes [eGovernment]

Eine derartige Entwicklung konnte man Ende der Sechziger nicht vorausahnen, doch schon damals stieß das Thema Datenschutz auf großes Interesse in der Bevölkerung, so dass im Zuge der Einführung der Rechner in die Behörden eine gesetzliche Regelung notwendig wurde.

Das erste Datenschutzgesetz der Welt

1974 war das Geburtsjahr des ersten Datenschutzgesetzes der Welt, das in Hessen verabschiedet wurde. Eine bundesweite Regelung schuf der Gesetzgeber 1977 mit dem „Bundesdatenschutzgesetz für die Verwaltung auf Bundesebene und für nichtöffentliche Stellen“. Darin heißt es über die Ziele des Gesetzes in §1 Artikel 1:

„Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.“

Man muss hier sehen, dass dies die weltweit erste Regelung zum Datenschutz war, es also noch keinerlei Erfahrungswerte gab. Als solche erreichte sie bei Weitem noch nicht das heutige Datenschutzniveau. Im zitierten Satz heißt es: „durch den Schutz personenbezogener Daten“ bei der Datenverarbeitung. Geschützt werden also die Dateien, auf die Erhebung der Daten geht das Gesetz nur unzureichend ein. Es wird der Umgang mit meinen personenbezogenen Daten wenn sie nicht mehr bei mir sind geregelt, nicht aber, was man von mir erfasst.

Dieser Mangel wurde 1983 offensichtlich, als die Kohl-Regierung eine umfassende Volkszählung plante. Im Zuge dessen sollte es zu einer Abgleichung der Bundesdaten mit den Landesmelderegistern kommen. Damit hätte es das gegeben, was die Alliierten nach dem Krieg bewusst verhindert hatten: ein zentrales Melderegister. Solch ein Register hat natürlich einen großen Nutzen, indem es zum Beispiel mühsame Anfragen an die Landesbehörden unnötig macht. Gleichzeitig legt es aber auch sehr viel Macht in die Hände derer, die Zugang haben, weil die Daten einer Volkszählung, wie wir gesehen haben, ja sehr umfangreich sind und die Möglichkeit der Korrelation im Rechner natürlich einfachst gegeben ist. Es gab wieder Proteste und es wurde eine Verfassungsbeschwerde in Karlsruhe eingereicht, die im gleichen Jahr zum „Volkszählungsurteil“ führte:

*„**Volkszählungsurteil 1983, Leitsätze (BVerfGE 65,1)***

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

[...]

5. Die in § 9 Abs. 1 bis 3 des Volkszählungsgesetzes 1983 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (§ 9 Abs. 4 VZG 1983) ist mit dem Grundgesetz vereinbar."

Wichtigster Punkt des Urteils ist Artikel eins. Darin wird der Datenschutz im Persönlichkeitsrecht des Grundgesetzes verankert. Das Verfassungsgericht stellt also heraus, dass das höchste deutsche Gesetz den Datenschutz einschließt. Das Recht auf „informationelle Selbstbestimmung" bedeutet, dass niemand meine Daten verarbeiten darf, ohne mich vorher zu fragen.

Artikel zwei regelt die Ausnahmen. Es wird erstens Normenklarheit gefordert, Ausnahmeregelungen müssen klar, verständlich und präzise abgefasst wird. Als Zweites wird Verhältnismäßigkeit gefordert, die Datenerhebung muss im Verhältnis zu ihrem Zweck stehen muss, was bedeutet, dass nicht zu viele Daten erhoben werden und diese nur für den entsprechenden Zweck zur Verfügung stehen. Die dritte Forderung ist die nach organisatorischen und verfahrenstechnischen Vorkehrungen, was bedeutet, dass für Transparenz bei der Verarbeitung und Datensicherheit auf technischer Ebene (Soft- und Hardware) gesorgt werden muss. [gehring et al. 2000]

Im Groben sind das auch die Grenzen des heute gültigen Datenschutzgesetzes, das in seiner ersten Form 1990 verabschiedet wurde, drei Jahre, nachdem die Volkszählung schließlich stattfand:

„Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird."

BDSG 1990 §1.1

Die Vorgaben des Volkszählungsurteils finden sich von da an also im Gesetz wieder. In der veränderten Fassung von 2001 (Umsetzung der EU-Datenschutzrichtlinie; siehe „Die europäische Union") ist es die heute gültige Grundlage des Datenschutzes in der Bundesrepublik.

Ich will kurz die wichtigsten Punkte des Gesetzes in der aktuell gültigen Fassung von 2001 erläutern. Das Erste ist wie bereits angeführt die Verankerung des Datenschutz im Grundgesetz. Desweiteren werden seit 1990 öffentliche und nichtöffentliche Stellen auf die gleiche Stufe gestellt und damit erstmals auch ein Datenschutz für Unternehmen gesetzlich vorgeschrieben. Das Gesetz vormals gültige Gesetz von 1977 war nur auf staatliche Institutionen gemünzt. Dieser Punkt ist sehr wichtig, weil es heute primär private Unternehmen wie Banken, Versicherungen oder gar professionelle Datenvermarktungsunternehmen (ein früher undenkbarer Dienstleistungszweig) sind, vor denen wir geschützt werden wollen/ müssen. In Anbetracht dessen, dass der Staat ja ein „Dienstleister an uns" ist, würde ich heute sogar dafür plädieren, noch einen Schritt weiter zu gehen und den Staat weniger zu restringieren als private Datenverwerter. Die Gefahren, die Kritiker einer solchen Lockerung sehen, nämlich, dass damit eine zu große Macht in die Hände des Staates gelegt wird, sehe ich zwar auch, aber ich denke, es ist abzuwägen. Ich werde noch

dazu kommen, aber gerade durch die Vernetzung heutiger Rechenzentren und Datenbanken ist es sowieso schon möglich, eine riesige Menge an Informationen über jeden Einzelnen von uns zu sammeln und derjenige, der dies illegal tut, stellt sicher eine größere Gefahr für uns dar als der Staat.

Das Gesetz schreibt weiterhin vor, dass so wenige Daten wie möglich gesammelt werden müssen. Wenn es schließlich aufgrund einer gesetzlichen Erlaubnis zur Datenerhebung kommt, so muss ich, wenn möglich, selbst nach der entsprechenden Auskunft gefragt werden. Außerdem sind mir umfassende Hinweise über den Zweck meiner Auskunft, das verarbeitende Unternehmen etc. zu machen. Weiterhin besteht eine Meldepflicht mir gegenüber, wenn Jemand meine Daten in nicht anonymisierter Form verwendet.

Das Gesetz regelt auch, dass ein Unternehmen, das Daten verarbeitet einen weisungsunabhängigen Datenschutzbeauftragten bestellen muss, dessen Aufgabe es ist, sich um die Belange der Personen zu kümmern, deren Daten verarbeitet werden. Das ist bemerkenswert, denn es zwingt ein Unternehmen dazu, Geld für etwas auszugeben, das ersteinmal keinen erkennbaren Nutzen bringt. Eigentlich ist es sogar ein Standortnachteil, denn wenn ich in Ländern arbeite, in denen es keine solchen Bestimmungen gibt, kann ich mir die Ausgaben für den/ die Mitarbeiter, die sich um den Datenschutz sorgen, sparen. Verarbeitet ein Unternehmen Daten aus Deutschland geht dies aber nicht, das Gesetz regelt hier nämlich, dass Länder, in denen meine Daten verarbeitet werden ein dem deutschen entsprechendes Schutzniveau bieten müssen. Für den Staat gibt es solch einen Datenschutzbeauftragten schon seit 1980. 1991, also ein Jahr nach Verabschiedung des BDSG, wurde das Bundesamt für die Sicherheit in der Informationstechnik eingerichtet, das die Förderung der Datensicherung zum Ziel hat. Der Staat unternimmt also einige Anstrengungen zum Datenschutz.

Einige bereichsspezifische Zusatzregelungen zum Bundesdatenschutzgesetz, die auf die Besonderheiten des jeweiligen Bereiches Bezug nehmen, finden sich in eigenen Gesetzen, wie zum Beipiel Brief-, Post- und Fernmeldegeheimnis. Speziell für den Bereich Desktop-PC, Netzwerke und Internet wurden 1993 im „Informations- und Kommunikationsdienstegesetz“ einige Zusätze verabschiedet:

- Pflicht zur *Datensparsamkeit*: „sammle nicht mehr Daten, als du unbedingt brauchst“
- Pflicht zur *Datentransparenz*: Dem Betroffenen muss unentgeltlich Einsicht in alle über ihn gesammelten Daten gegeben werden und ihm muss offen gelegt werden, wie und von wem seine Daten verwendet werden.
- *Einwilligungspflicht* des Betroffenen: „Ich bin damit einverstanden, dass sie meine Adresse speichern“ (Gewinnspiele, Abos, Kundenprofile, ...)

Wie wir gesehen haben finden sich diese drei wichtigen Kernpunkte des Datenschutz auch im BDSG von 2001 wieder. In der Fassung von 1990 waren sie in dieser Ausprägung noch nicht vorhanden. Daran zeigt sich eine Entwicklung: Man geht dazu über, das deutsche Datenschutzrecht zu vereinfachen. Es haben sich viel zu viele Sonderregelungen und Ausnahmen angesammelt. Um zu entscheiden, ob eine Verarbeitung erlaubt ist müssen viele Gesetze durch-

forstet werden und das kostet Zeit und damit für ein Unternehmen Geld und bringt auch für uns als Betroffene keinen Vorteil, weil wir nicht nur durch die verklausulierten Gesetzestexte, sondern auch durch die riesige Fülle von Gesetzen den Überblick verlieren und deshalb gar nicht wissen, wann wir wo auf unsere Rechte pochen können.

Die europäische Union

Auch in anderen Ländern wurden nach 1977 Normen zum Datenschutz geschaffen und 1995 wurde in Amsterdam im Rahmen der Harmonisierung der Gesetze innerhalb der Union die EU-Datenschutzrichtlinie verabschiedet. Diese muss in allen EU-Mitgliedsländern in die Gesetze übernommen werden und stellt somit den Mindestdatenschutz innerhalb des Staatenbundes dar. Sie enthält folgende Kernpunkte:

- Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare
- Ein Höchstmaß an Transparenz gegenüber den Betroffenen
- Kontrolle der Einhaltung durch Einzelne, den Staat und unabhängige Verbände etc.

Innerhalb der EU gibt es also verbindliche Gesetze, die den Bürger vor willkürlicher Nutzung seiner Daten —und damit einem erheblichen Eingriff in seine Privatsphäre— schützen. Da Gesetze aber nur territorial Geltung haben, könnte man einfach seine Daten in ein Nicht-EU-Land (z.B. China) exportieren, dort verarbeiten und anschließend wieder einführen. In Deutschland haben wir gesehen, geht dies nicht, weil es gesetzlich verboten ist. Das war auch schon in der alten Fassung, also vor Umsetzung der EU-Richtlinie, so. Damit dies in keinem Mitgliedsland geschieht, schützt sich die europäische Union durch das „Safe Harbour“-Prinzip: Daten aus der EU dürfen nur in Länder exportiert werden, die von der EU als sicherer Hafen für Daten eingestuft werden, also selbst durch eigene Gesetze ein ausreichend hohes Schutzniveau gewährleisten.

Dieses Prinzip hat noch einen anderen Zweck: Wenn alle Länder, die mit der EU handeln, deren Datenschutzrichtline erfüllen müssen, wird diese implizit zum Weltstandard und das liegt durchaus im Interesse der Union.

Nordamerika als wichtiger Handelspartner ist von der dortigen Gesetzessituation her kein Safe Harbour, denn dort hält man es mit dem Datenschutz völlig anders.

Die USA

Getreu dem Motto „Jeder ist seines Glückes Schmied“ ist auch jeder seiner Daten Schützer.

Es gibt praktisch keinen staatlichen Datenschutz. Stattdessen gilt wie in vielen Bereichen das Prinzip der Selbstregulierung des Marktes. Es gibt so genannte „Codes of Conduct“, Verhaltensregeln, die sich die Unternehmen selbst geben. Dazu schließen sie sich mit anderen Unternehmen zu sogenannten Trusts zusammen, die sich dann an die gemeinsamen Datenschutzrichtlinien halten und so um das Vertrauen des Kunden werben.

Die USA wurden daher auch erst nach Abschluss einiger bilateraler Zusatzabkommen mit der EU, die nur auf Drängen diverser Unternehmen zustande kamen, als Safe Harbour eingestuft.

Datenschutz in Zeiten der Globalisierung

Für die Wirtschaft gibt es heute fast keine Grenzen mehr. Erst recht nicht, wenn es um die Datenverarbeitung geht.

Die digitale Speicherung ermöglicht es früher unvorstellbare Mengen an Daten z.B. auf einer CD zu transportieren, verlustfrei zu kopieren, zu manipulieren et cetera.

Die Geschwindigkeit heutiger Prozessoren erlaubt es, immense Mengen an Daten in verschwindend geringer Zeit zu verarbeiten.

Das Internet verbindet weltweit Standorte in einer nie erreichten Geschwindigkeit und es macht daher technisch keinerlei Unterschied mehr, wo die Daten gespeichert, wo sie verarbeitet und wo das Ergebnis dann letztlich genutzt wird.

Da stellt sich die Frage, wie denn ein effizienter Datenschutz heute aussehen kann.

Wir haben beide Seiten gesehen, einerseits Europa und besonders Deutschland mit vielen Gesetzen zum Datenschutz und auf der anderen Seite Nordamerika mit einer Art „Datenschutz-Anarchie“.

Als in Deutschland lebender Mensch könnte man zu der Auffassung kommen: So wie es hier ist, ist es doch gut, warum machen es nicht alle so? Selbst Datenschutzexperten sehen das nicht so. Ich habe es schon angedeutet: Wie in vielen Bereichen gibt es hierzulande auch bei der Rechtsprechung eine Tendenz zur Überregulierung. In Deutschland gilt der Hang zum Gesetzesperfektionismus: Für jede Ausnahme muss es ein Gesetz geben. Und genau das ist das Problem. Aus dem ursprünglichen Gedanken, dass die persönlichen Daten grundsätzlich geschützt sind und nur in Ausnahmefällen verwendet werden dürfen, ist eine Regelung mit tausenden von Spezialfällen geworden, die den Datenschutz da und dort regeln und überall, wo man kein Gesetz findet, verwendet man die Daten einfach, denn wo kein Kläger ist, gibt es auch kein Gesetz und der Datenschutz ist nicht so einfach zu kontrollieren. Das deutsche System ist dadurch, dass es so aufwendig ist, zu einem Wettbewerbsnachteil für Unternehmen geworden. Die Überprüfung, ob eine Verarbeitung rechtmäßig ist, dauert viel zu lange und wird deshalb wohl oft erst gar nicht vorgenommen.

Damit zusammen hängt auch das Problem der Trägheit der Legislative. Der Gesetzgebungsprozess ist viel zu langsam, um auf die Dynamik des Marktes reagieren zu können. Salopp gesprochen sind die Daten schon verarbeitet, bis überhaupt ein Antrag auf ein Gesetz zum entsprechenden Verbot eingereicht werden kann.

Ein weiteres Problem von Gesetzen ist, dass sie ihre Anwendung nur im entsprechenden Land finden. Es gibt keinen Weltgerichtshof mit Weltpolizei, der für die Durchsetzung irgendwelcher weltweit geltender Normen sorgt. Sie können sich —wie die Menschenrechte— nur durchsetzen, wenn sie einen breiten Konsens finden und fast alle Staaten sie ratifizieren. Wie wir gesehen haben, postuliert die EU mit dem Safe Harbour-Prinzip solch eine Lösung: Wer mit uns Daten verarbeiten will muss unsere Standards erfüllen und besser noch in seine Gesetze übernehmen.

Mit Ländern, die ein völlig anderes Verständnis vom Datenschutz haben, wie beispielsweise den USA, wird dies aber nicht funktionieren, weil sie die Gesetze einfach nicht übernehmen werden, was für die dort ansässigen Unternehmen momentan sogar ein Wettbewerbsvorteil sein kann, weil sie den vielen zusätzlichen Aufwand des Datenschutz, der ja erstmal keinen erkenntlichen Gewinn abwirft, eben nicht haben. Und auch das ist ein sehr entscheidender Punkt: Es gibt momentan keinen marktwirtschaftlich erkennbaren Nutzen von Datenschutz. Kaufentscheidend ist der Preis. Welchen Datenschutzstandard ein Unternehmen erfüllt habe ich ehrlich gesagt noch nie in meine Kaufentscheidung einbezogen.

Will ich denn überhaupt Datenschutz? Und will ich ihn immer noch, wenn ich dafür mehr bezahlen muss? Der BigBrother-Teilnehmer will ihn vielleicht nicht, oder will er ihn doch und hat sich nur bewusst in diesem Fall entschieden, sein Privatleben für ein paar Wochen aufzugeben? Ist der Datenschutz heutzutage etwas, das uns bewusst ist? Ich würde sagen: Noch immer eher nicht, denn was passiert denn schlimmes, wenn wir unsere Daten preisgeben? Es kommt kein Wahnsinniger, der uns, weil wir nicht seiner Rassenideologie entsprechen, in ein Konzentrationslager steckt. Wir bekommen nur „zielgerichtete“ Werbung in den Briefkasten, das ist doch nett... oder? Wir bekommen keine Absage auf unser Jobgesuch, nur weil wir bei unserer alten Arbeitsstelle auffällig oft am Montag krank waren, denn das weiß ja keiner...

Wenn wir in den USA leben würden, wäre es gut, wenn der Datenschutz und vor allem die Grenze von dem, was wir preisgeben wollen, uns bewußt wären, denn dort schützt uns nicht der Staat. Dort müssen wir selbst mündig sein.

Die „Anarchie“ oder positiver ausgedrückt Selbstregulierung ist doch positiv. Der Markt stellt seine Schutzregeln selbst auf, also kann er sich flexibel und schnell an seine eigenen Veränderungen anpassen und wenn die Regeln schlecht für uns sind, können wir den Markt ja bestrafen, indem wir ihn beukottieren. Das ist Marktwirtschaft. Doch funktioniert das? Ich war nie in den USA und kann deshalb nicht aus Erfahrung sprechen, doch wieso sollte der Markt, also konkreter ein Unternehmen, das etwas anbietet und seinen Profit maximieren will Regeln aufstellen, die ihm Kosten verursachen oder Mühe machen? Würde ich das Unternehmen beukottieren, wenn es einen „schlechten“ Datenschutzstandard hat? Nein, weil ich mir gar nicht

die Mühe machen würde, mich zu informieren, welche Regelungen das Unternehmen im Detail aufgestellt hat und was diese für mich bedeuten. Aber vielleicht bin ich das einfach noch nicht gewöhnt. In meinem Land gibt es ja Mindeststandards und einen Mindest- oder vielleicht treffender Fast-Rundumschutz. Ich glaube, ich bin bei diesem Thema noch etwas zu unmündig... aber so wie es ist, geht es, wie wir gesehen haben auch nicht weiter und wie im „wilden Westen“ wollen wir es eigentlich auch nicht.

Also, was ist die Lösung? Vielleicht ein goldener Mittelweg: So viel Freiheit wie möglich bei gleichzeitig so viel Schutz wie nötig. Wir können nicht erwarten, dass jeder Bürger zum Datenschutzexperten wird und sich ganz alleine sicher auf dem Ozean der Datenpiraten zurechtfinden kann. Aber wir können dem Bürger schon mehr Selbstverantwortung geben. Ich glaube es würde ausreichen, ein paar Mindeststandards gesetzlich festzulegen und ansonsten als Staat Empfehlungen und Anreize zu einem geeigneten Datenschutz zu geben.

Ein auch von der EU geförderter Versuch dazu findet gerade in Schleswig-Holstein statt. Dort gibt es ein so genanntes „Datenschutzaudit“ für öffentliche Stellen. Grob gesagt ist das eine Art Gütesiegel für eine öffentliche Institution, das ihr bescheinigt, Anstrengungen in die richtige Richtung beim Datenschutz zu unternehmen. Die beantragende Stelle macht dazu zuerst eine Bestandsaufnahme des zu auditierenden Prozesses, legt dann selbst die Datenschutzziele fest und richtet schließlich ein Datenschutzmanagementsystem ein, mit dem es das Erreichen der Ziele überwacht. Anschließend fasst die Stelle darüber eine Datenschutzerklärung ab, in der sie die einzelnen Schritte erläutert. Diese Erklärung wird vom Unabhängigen Landeszentrum für Datenschutz (ULD) geprüft und eventuell ergänzt und verbessert. Bei positiver Prüfung hat die Stelle das Audit bestanden und kann fortan drei Jahre damit werben, dann muss sie sich erneut auditieren lassen.[körffer2002]

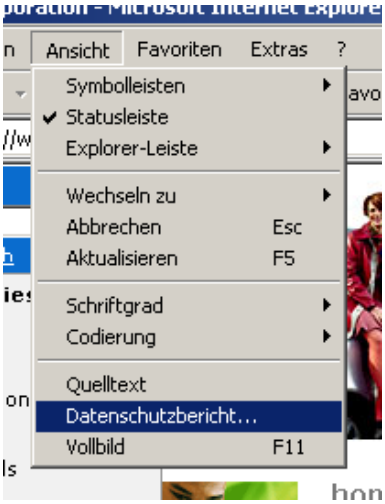
Datenschutzaudit-Siegel für zertifizierte Behörden

Entsprechend gibt es auch ein Zertifikat für Hard- und Software zur Datenverarbeitung in öffentlichen Stellen. Um das Zertifikat zu erhalten, muss man sein Produkt von einem unabhängigen bei der ULD akkreditierten Sachverständigen begutachten lassen. Werden alle Anforderungen vom ULD als erfüllt betrachtet, bekommt man das Zertifikat und kann anschließend zwei Jahre damit werben.[schleswig]

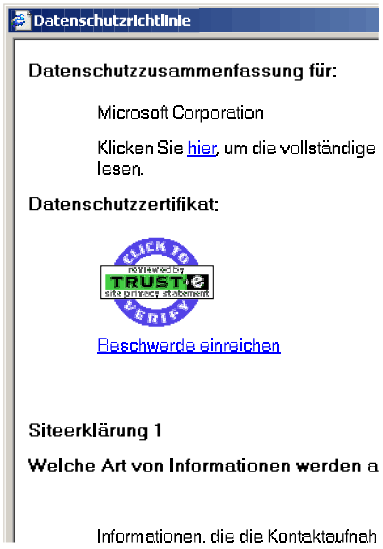
Datenschutzaudit-Siegel für zertifizierte Hard- und Software

Idealerweise soll es irgendwann so sein, dass der Markt solche Unternehmen und Produkte favorisiert, die eine Auszeichnung erhalten haben. In Schleswig-Holstein leitet das Land seine Behörden dazu an, indem es den Einsatz solcher Produkte empfiehlt. Bei Akzeptanz durch den Markt würde das Siegel zum Standortvorteil und der Datenschutz damit zu einem auch wirtschaftlich lohnenden Faktor bei der Produktion, was ihn in jedem Unternehmen von einem leichten Schattendasein ins Rampenlicht stellen würde. Wenn das funktioniert, ist das Audit ein großer Schritt in die richtige Richtung.

Wichtig bei der Einführung solcher Bewertungssysteme wäre mir in jedem Fall eine einheitliche Regelung über die Vergabekriterien und auch ein einheitliches Symbol. Denn, wenn jeder sein eigenes Gütesiegel vergibt, nützt mir dies als Verbraucher am Ende wenig, da ich dann trotzdem jedesmal prüfen muss, was das Zeichen aussagt.



Wenn die Seite P3P unterstützt, ist der Menupunkt „Datenschutzbericht“ im Menu „Ansicht“ des IE 6 verfügbar. Beispiel: www.microsoft.com.



Das Audit ist ein Schritt in Richtung amerikanisches System, ein Schritt weg von der totalen staatlichen Regelung, hin zur Selbstregulierung (mit staatlicher Lenkung).

Auch von der anderen Seite des Ozeans werden Schritte auf einen Mittelweg zu gegangen. Das WorldWideWeb-Consortium (W3C; Internet-Normungsgremium mit weltweiten Mitgliedern) beispielsweise ist gerade dabei, einen Standard zu schaffen, der den Datenschutz in einem System, in dem jeder seine eigenen Regeln hat, für den Verbraucher wieder handhabbar macht. Das Privacy Preferences Project (P3P; http://www.w3.org/TR/P3P/) sieht vor, dass zu jeder Seite im Netz, die datenschutzrelevante Informationen enthält oder verarbeitet, ein standardisiertes Formular vom Anbieter bereitgestellt werden kann, welches die Datenschutzrichtlinien der Seite in einem standardisierten Format erläutert.

Konkret bedeutet dies, dass der Nutzer eine entsprechende Software installiert, die die Formulare ausliest und sich einmal damit auseinandersetzt, wie viel Datenschutz er will. Fortan muss er sich idealerweise nicht mehr um den Datenschutz kümmern: Da jede Seite eine Datenschutzsignatur hat, kann der Browser diese mit dem einmal eingestellten Profil abgleichen und auf Probleme aufmerksam machen, also sagen, wenn eine Seite gegen eine von meinen Einstellungen verstößt. Riesiger Vorteil bei der Lösung ist, dass der Anwender nicht ständig auf den Datenschutz bedacht sein muss und ihn aus Überforderung irgendwann ignoriert. Er stellt einmal seine Vorgaben ein und surft dann automatisch so sicher, wie er es gewünscht hat. Positiver Effekt davon sollte sein, dass die Unternehmen versuchen, mit den Einstellungen möglichst vieler Benutzer konform zu bleiben, damit diese keine abschreckenden Hinweise zur Verletzung ihrer Datenschutzrichtlinie bekommen und sich damit ein einheiliches am Konsumenten orientiertes Datenschutzniveau einstellt.

An P3P zeigen sich sehr gut die unterschiedlichen Geschwindigkeiten, mit denen auf der einen Seite der Markt und auf der anderen Seite der Staat Lösungen realisiert. In den aktuellen Browserversionen von Microsoft und Netscape (IE 6/ Netscape 7) ist P3P bereits integriert (siehe links; Vorschlag des w3 stammt vom 16.4.2002), wenn die Einstellungsmöglichkeiten des Internet Explorers sich bisher auch nur auf Cookies, also vom Server auf meinem Rechner gespeicherte Informationen, beziehen. Für eine sinnvolle Nutzung des Konzeptes bedarf es vor allem Einstellungsmöglichkeiten für Formulare, wie sie beispielsweise Webshops verwenden. Diese Formulare könnten dann sogar automatisch ausgefüllt werden, weil ich als Nutzer mir ja sowieso überlegt habe, dass ich bereit bin, meine Daten preiszugeben. Diese Erweiterung wird aller Voraussicht nach schneller Einzug in unser tägliches Leben erhalten als die staatlich kontrollierten Zertifikate.

Eine Frage konnte ich in meinen ganzen Ausführungen nicht beantworten: Wie viel Datenschutz wollen wir denn?

Vielleicht liegt das daran, dass es keine pauschale Antwort gibt...

Fazit

Die heutige Gesellschaft ist eine Dienstleistungs- und Informationsgesellschaft. Das Sammeln von Daten hat in den letzten dreißig Jahren immens zugenommen, enorm beschleunigt durch die Entwicklung des Internet in den letzten zehn Jahren. Dabei ist der ursprüngliche Datensammler, der Staat, heute zu einer eher geringen Gefahr für unsere Privatsphäre geworden. Diese wird heute viel eher von privaten Unternehmen wie Banken, Versicherungen, Marketingunternehmen etc. beschnitten. Gerade durch die Globalisierung geraten wir immer mehr in die Position des (gezwungenermaßen) mündigen Konsumenten, der sich selbst klar werden muss, wo er den Kreis um sich zieht.

Ich glaube, der Weg aus dem „Schutz des Laufstalls“ in die freie Welt findet in Deutschland gerade statt und das wird uns in absehbarer Zeit noch bewusster werden: Einerseits haben wir sehr viel Datenschutz, der zu fast jeder Datenverarbeitung unser ausdrückliches Einverständnis erfordert (da eine umfassende Kontrolle nicht möglich ist, scheint dies vielleicht nicht so, anderweitige Datenverwertung ist aber illegal und kann angezeigt werden), andererseits können wir aber auch dieses Einverständnis geben und den Markt an unserem Privatleben teilhaben lassen —sei es durch Fragebögen (z.B. auch Payback-Systeme) oder die Teilnahme bei der Fernsehserie Big-Brother.

Es wird wohl noch eine Weile dauern, bis der Datenschutz sich als etwas ganz normales, uns aber durchaus auch bewusstes etabliert hat und auch, bis sich eine Linie erkennen lässt, wie viel Datenschutz „das Volk“ will.

Die Einführung von Zertifikaten gibt uns beispielsweise die Möglichkeit „demokratisch“ über unsere Kaufentscheidung mitzuteilen, was uns der Datenschutz wert ist. Der gleiche Weg wird mit der Akzeptanz von P3P im Internet beschritten werden.

Das zeigt, dass der Datenschutz gerade weltweit ein Thema ist, nicht nur bei uns. Wir müssen uns zusehends selbst aktiv für unseren Datenschutz einsetzen, indem wir zum Beispiel P3P benutzen. Nur durch verstärkte Nachfrage wird das Angebot größer werden.

Auf dem Sektor des Datenschutz wird sich in nächster Zeit wohl noch einiges tun —hoffentlich in für uns positivem Sinn!

Marc-Oliver Pahl, Juni 2003

Quellen

Meine Hauptquelle war: Johann Bizer, Bernd Lutterbeck, Joachim Rieß, Umbruch von Regelungssystemen in der Informationsgesellschaft: Freundesgabe für Alfred Büllesbach, Steinkopf-Verlag Stuttgart 2002, http://www.alfred-buellesbach.de

vor allem folgende Artikel (in der Reihenfolge des Buches):

- Umbruch von Regelungssystemen - Johann Bizer, Bernd Lutterbeck, Joachim Rieß
- Datenschutz im Unternehmen – eine Gratwanderung zwischen Persönlichkeitsschutz und bürokratischer Geschäftsbeschränkung/ Manfred Gentz
- Die Wissensgesellschaft bauen! - Bernd Lutterbeck
- Informationsrecht in der Informationsgesellschaft - Thomas Dreier
- Marktwirtschaftlicher Datenschutz - Helmut Bäumler
- Modernisierung des Datenschutzrechtes – eine Art Zwischenbilanz - Jörg Tauss
- Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive - Alexander Roßnagel
- Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? Zum Modernisierungsgutachten 2002 für den Bundesminister des Inneren. - Wolfgang Kilian
- Big Brother und die schöne neue Welt der Vermarktung personenbezogener Informationen - Bettina Sokol/Roul Tiaden
- Der Code – gestaltbar für und gegen den Datenschutz - Johann Bizer
- Daten- und Persönlichkeitsschutz im Zeitalter der Globalisierung Philosophische Bausteine für eine interkulturelle Begründung - Otfried Höffe

[born]: Sigrid Born, Datenschutz in Deutschland, Goethe-Institut Inter Nationes, http://www.goethe.de/kug/ges/rch/thm/de17135.htm, Stand: 1/ 2003

[computer]: „Computer“, www.referate.heim.at/referate/html/comput02.html, Stand: 1/ 2003

[dietschi]: Andreas Dietschi, Mekmale für Hochkulturen, www.dsg.ch/hochkult.htm, Stand: 1/ 2003

[eGovernment]: „eGovernment Initiative der Bundesregierung“, http://www.bund.de/BundOnline2005-.6164.htm, Stand: 1/ 2003

[gehring et al. 2000]: Robert Gehring, Kei Ishii, Bernd Lutterbeck, Vorlesungsscript zu „Information Rules“, Technische Universität Berlin, WS 00/01, ig.cs.tu-berlin.de/w2000/ir1/t11-01/ + /t11-02/, Stand: 1/ 2003

[golaSchomerus2002]: Peter Gola, Rudolf Schomerus, Bundesdatenschutzgesetz: BDSG, Kommentar, 7. Auflage, Beck-Verlag München 2002

[hoeren2002]: Thomas Hoeren, Grundzüge des Internetrechts: E-Commerce, Domains, Urheberrecht, 2. Auflage, Beck-Verlag München 2002

[ishii et al. 2000]: Robert Gehring, Kei Ishii, Bernd Lutterbeck, Vorlesungsscript zu „Information Rules“, Technische Universität Berlin, WS 00/01, ig.cs.tu-berlin.de/w2000/ir1/t11-01/vz-leitsaetze.html, Stand: 1/ 2003

[karlsruhe1983]: „Volkszählung“, „Vernummerung“ und Datenerfassung bei den Nazis, Karlsruher Stadtzeitung Nr.30 Frühling 83, www.trend.partisan.net/trd7899/t507899.html, Stand: 1/ 2003

[knoop2002]: Prof. Dr. H.-B. Knoop, Vorlesungsscript zu „Ausgewählte Kapitel zur Geschichte der Mathematik“, Gerhard-Mercator-Universität Duisburg, WS 02/ 03, www.uni-duisburg.de/FB11/LEHRE/W02/GESCHICHTE/g01.pdf (Entwicklung der Zahlensysteme), Stand: 1/ 2003

[körffer2002]: Barbara Körffer, Unabhängiges Landeszentrum für Datenschutz in Kiel, Das schleswig-holsteinische Datenschutz-Behördenaudit, Kiel Sommerakademie 2002, http://www.datenschutzzentrum.de/somak/somak02/sak02koe.htm, Stand: 1/ 2003

[langPauli2002]: Hartmut Lang, Julia Pauli, Der ethnographische Zensus. Eine praxisorientierte Einführung, 2002, www.methoden-der-ethnographie.de/heft2/ECensus.pdf

[lorenz et al.]: Rüdiger Lorenz et al., Geschichte des Römischen Reiches, www.pinselpark.de/geschichte/tabellen/a753p744_rom1.html, Stand: 1/ 2003

[lutterbeck et al. 2000]: Robert Gehring, Kei Ishii, Bernd Lutterbeck, Vorlesungsscript zu „Information Rules“, Technische Universität Berlin, WS 00/01, http://ig.cs.tu-berlin.de/w2000/ir1/t12-01/, Stand: 1/ 2003

[neßler2001]: Volker Boehme-Neßler, CyberLaw : Lehrbuch zum Internet-Recht, Beck-Verlag München 2001

[pfeiffer]: Udo R. Pfeifer, Kleiner Geschichtsabriss zur Computer-, Technik-, Kommunikations - und Medien-geschichte, ods.dokom.net/mbr/2020/geschichte.htm, Stand: 1/ 2003

[schleswig]: Häufig gestellte Fragen zum Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Daten-schutz Schleswig-Holstein, http://www.datenschutzzentrum.de/faq/g-siegel.htm, Stand: 1/ 2003

[seiffert2002]: Wilfried Seiffert, Landesbeauftragter für den Datenschutz Niedersachsen 2001/ 2002, „Der Daten-schutz in den Jahren 2001 und 2002“, http://www.lfd.niedersachsen.de/master/0,,C1372769_N13128_L20_D0_I560,00.html, Stand: 1/ 2003

[tinnefeldEhmann1998]: Marie-Therese Tinnefeld und Eugen Ehmann, Einführung in das Datenschutzrecht, 3. Auflage, Oldenbourg-Verlag München, Wien 1998