

Stichwort: **Datenschutz**

Die folgenden Texte wurden Wikipedia, der freien Enzyklopädi entnommen und nur formatiert, um sie dem Erscheinungsbild unserer Seiten anzupassen. Alle Links und Verweise, innerhalb dieses Dokumentes und wenn sie nicht auf Seiten von digitalDokumente.com führen, unterliegen dem Urteil vom 12. Mai 1998 in dem das Landgericht Hamburg entschieden hat, daß man durch die Ausbringung eines Links die Inhalte der gelinkten Seite ggf. mit zu verantworten hat. Dies kann - so das Landgericht - nur dadurch verhindert werden, daß man sich ausdrücklich von diesen Inhalten distanziert.

Datenschutz ist ein aus dem 20. Jahrhundert stammender Begriff, der ursprünglich den Schutz personenbezogener Daten vor Mißbrauch zum Inhalt hatte. Der Begriff wurde gleichgesetzt mit *Schutz der Daten*, *Schutz vor Daten* oder auch *Schutz vor Verdattung*.

Heute wird der Zweck des Datenschutzes darin gesehen, den Einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, daß jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen.

Die Bedeutung des Datenschutzes ist auf Grund der technischen Entwicklung einerseits (Stichworte: Internet, E-Mail, Mobiltelefone, Videoüberwachung, Data Warehouse) und des erhöhten Informationsbedürfnisses staatlicher Stellen und privater Unternehmen andererseits (Stichworte: Rasterfahndung, Mitarbeiterüberwachung, Kundenprofile, Auskunfteien) stetig gestiegen. Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat.

Vor allem durch die weltweite Vernetzung der Computer durch das Internet sind sehr große Gefahren hinsichtlich des Schutzes personenbezogener Daten hinzugekommen. Datenschützer müssen sich deshalb mit den grundlegenden Fragen von Datensicherheit auseinandersetzen, wenn Datenschutz wirksam sein soll.

Internationale Regelungen

Seit 1980 existieren mit den OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data international gültige Richtlinien, die die Ziele haben, die mitgliedstaatlichen Datenschutzbestimmungen weitreichend zu harmonisieren, einen freien Informationsaustausch zu fördern, ungerechtfertigte Handelshemmnisse zu vermeiden und eine Kluft insbesondere zwischen den europäischen und US-amerikanischen Entwicklungen zu verhindern.

1981 verabschiedete der Europarat mit der Europäischen Datenschutzkonvention eines der ersten internationalen Abkommen zum Datenschutz. Die Europäische Datenschutzkonvention ist bis heute in Kraft und besteht unabhängig von den Datenschutzrichtlinien der Europäischen Union.

Strukturelle Unterschiede USA / EU

Zwischen den USA und der EU gibt es im Bezug auf den Datenschutz strukturelle Unterschiede: Während die EU im Wege einer systematischen Gesetzgebung ein gesetztes Recht geschaffen hat, gibt es in den USA eine anlaßbezogene Gesetzgebung, die bestimmte Fälle regelt.

In der EU sind durch das Verbotprinzip mit Erlaubnisvorbehalt nur bestimmte Datenverarbeitungen erlaubt, während in den USA nur bestimmte Datenverarbeitungen verboten sind und man sonst im Wesentlichen auf den Markt und freiwillige Selbstverpflichtungen der Wirtschaft vertraut.

Nach deutschem und europäischem Datenschutzrecht ist ein Transfer von Daten in die USA eigentlich ausgeschlossen, weil dort ein ausreichendes Schutzniveau nicht erreicht ist. Dies trifft amerikanische Unternehmen, die von den jeweiligen Datenschutzgesetzen z. B. in Deutschland erfaßt werden, weil sie Daten hier erheben oder verarbeiten. Aus diesem Grund wurde mit den USA ein Abkommen geschlossen, wonach dort Unternehmen, die sich selbst zu einem bestimmten Schutz verpflichten, in eine Liste der so genannten *Safe Harbors* (deutsch: "sichere Häfen") eingetragen werden. Diese Unternehmen dürfen Daten dann auch in der EU erheben und verarbeiten. Es handelt sich um eine freiwillige Selbstverpflichtung, die jedoch bindend ist. Das Datenschutzniveau der EU wird dadurch aber nicht vollständig gewährleistet.

Europäische Union

Mit der *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* haben das Europäische Parlament und der Europäische Rat Mindeststandards für den Datenschutz der Mitgliedsstaaten festgeschrieben. Geregelt wird insbesondere auch die Übermittlung von personenbezogenen Daten in Drittstaaten, die nicht Mitglied der EU sind: Gemäß Artikel 25 ist die Übermittlung nur dann zulässig, wenn der Drittstaat ein *angemessenes Schutzniveau* gewährleistet. Die Entscheidung, welche Länder dieses Schutzniveau gewährleisten, wird von der Kommission getroffen, die dabei von der so genannten Artikel-29-Datenschutzgruppe beraten wird. Aktuell (Stand 9/2004) wird gemäß Entscheidung der Kommission bei folgende Drittstaaten ein angemessenes Schutzniveau gewährleistet: Schweiz, Kanada, Argentinien, Guernsey, Insel Man, bei der Anwendung der vom US-Handelsministerium vorgelegten Grundsätze des "sicheren Hafens" sowie bei der Übermittlung von Fluggastdatensätzen an die US-Zoll- und Grenzschutzbehörde (CBP).

Insbesondere die Entscheidung über die Zulässigkeit der Übermittlung von Fluggastdatensätzen an die US-amerikanischen Zollbehörden ist stark umstritten gewesen. So hat das Europäische Parlament gegen diese Entscheidungen der Kommission und des Rates Klage eingereicht, da es seiner Ansicht nach unzureichend beteiligt worden sei und zudem seitens der USA kein angemessenes Datenschutzniveau garantiert werde.

Ergänzt wurde diese Richtlinie durch die bereichsspezifischere *Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation*. Nachdem die Umsetzungsfrist der Richtlinie am 31. Dezember 2003 abgelaufen war, wurde gegen neun Mitgliedsstaaten ein Vertragsverletzungsverfahren eingeleitet; nachdem nur Schweden die Richtlinie daraufhin vollständig umgesetzt hat, droht Belgien, Deutschland, Griechenland, Frankreich, Luxemburg, den Niederlanden, Portugal und Finnland ein Verfahren vor dem Europäischen Gerichtshof.

Datenschutzportal der europäischen Kommission (http://europa.eu.int/comm/internal_market/privacy/index_de.htm)

aus Wikipedia, der freien Enzyklopädi

Richtlinie 95/46/EG als PDF (http://141.3.20.23/datis/data/RL_eu_datenschutz_de_809.pdf)

Richtlinie 2002/58/EG als PDF (http://europa.eu.int/eur-lex/pri/de/oj/dat/2002/l_201/l_20120020731de00370047.pdf)

Bundesrepublik Deutschland

In der Bundesrepublik Deutschland regelt das Bundesdatenschutzgesetz (BDSG) die gesetzlichen Bestimmungen zum allgemeinen Datenschutz für die Wirtschaft und Bundesbehörden. Es wird durch unter anderem folgende bereichsspezifischere Regelungen ergänzt:

für Landesbehörden sind die Landesdatenschutzgesetze (LDSG) zuständig

für Teledienste das Teledienstedatenschutzgesetz (TDDSG)

für Mediendienste der Staatsvertrag über Mediendienste

für den Bereich Telekommunikation durch die Telekommunikations-Datenschutzverordnung (TDSV)

Durch das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 erhielt das Recht auf informationelle Selbstbestimmung und damit der Datenschutz Verfassungsrang.

Neben dem BDSG und den Landesdatenschutzgesetzen gibt es eine Reihe speziellerer Gesetze, die (unter anderem auch) dem Datenschutz dienen und dem BDSG vorgehen (etwa das Sozialgesetzbuch X für den Schutz von Sozialdaten, Strafgesetzbuch für ärztliche Schweigepflicht, die Abgabenordnung für das Steuergeheimnis ...)

Entwicklung

George Orwell zeigte schon 1948 in seinem Roman "1984" die Dystopie eines totalitären Überwachungsstaates.

Durch weltweite Überwachungssysteme wie Echelon, durch die massiv erweiterten Befugnisse von Polizei und Geheimdiensten nach den Terroranschlägen vom 11. September 2001, durch wachsende Datenbanken von Unternehmen und staatlichen Einrichtungen gekoppelt mit immer größeren Speicherkapazitäten und schnelleren Verarbeitungsmöglichkeiten sowie durch immer massivere Videoüberwachung und die Aushöhlung des Brief- und Postgeheimnisses, sehen viele Datenschützer - wie der Chaos Computer Club und die Deutsche Vereinigung für Datenschutz (DVD) e.V. - den Datenschutz in Deutschland und weltweit massiv gefährdet.

Literatur

Bäumler, Dr. Helmut. *Datenschutz im Internet* <http://www.datenschutzzentrum.de/somak/somak00/baeumler.htm>

Christiane Schulzki-Haddouti: *Bürgerrechte im Netz* (http://www.bpb.de/publikationen/UZX6DW,,0,B%FCrgerrechte_im_Netz.html), Bundeszentrale für politische Bildung, ISBN 3810038725

Christiane Schulzki-Haddouti: *Vom Ende der Anonymität. Die Globalisierung der Überwachung.* (http://www.heise.de/tp/deutsch/html/buch_1a.html) ISBN 3882291850

Christiane Schulzki-Haddouti: *Datenjagd. Eine Anleitung zur Selbstverteidigung.* ISBN 3434530894

Heinzmann, Peter L.: *Das Internet- ein Datenschleppernetz" für Personendaten?* Aus: *Das Internet- Ende des Datenschutzes?* Symposium 1997. Materialien zum Datenschutz Nr. 24 <http://www.datenschutz-berlin.de/infomat/dateien/Symp97.pdf>

Peter-Alexis Albrecht: *Die vergessene Freiheit. Strafrechtsprinzipien in der europäischen Sicherheitsdebatte.* ISBN 3830503555.

Herausgegeben von Helmut Bäumler, Astrid Breinlinger und Hans-Hermann Schrader: *Datenschutz von A-Z.* Loseblattwerk, 1 Ordner, z. Zt. ca. 1162 Seiten, Luchterhandverlag. [Inhaltsverzeichnis mit Leseprobe](#)

Selbstdatenschutz bedeutet, die Gefahren hinsichtlich Datenschutz und Datensicherheit kennenzulernen und selbst aktiv Gegenmaßnahmen zu ergreifen.

Insbesondere durch die weltweite Vernetzung gibt es in Bezug auf personenbezogene Daten neue Bedrohungen in bis dahin niemals gekanntem Ausmaß. Problematisch ist an der Internettechnologie vor allem, daß sie bereits einen sehr hohen Komplexitätsgrad erreicht hat. Selbst einzelne Fachleute sind heute nicht mehr in der Lage, die gesamte Technik zu überblicken.

Durch weitere Neuentwicklungen dieser Technik steigert sich die Komplexität von Tag zu Tag.

Im Gegensatz dazu kennen die meisten Verbraucher die Gefahren nicht, die damit verbunden sind, persönliche Daten herauszugeben. Erschwerend kommt hinzu, daß die meisten Internetnutzer der fälschlichen Meinung sind, das Internet wäre anonym. Sie sind sich der Bedrohungen eines in Wirklichkeit "offenen Netzes" nicht bewußt.

In einer Informationsgesellschaft bedarf es somit der Aufklärung und entsprechender Bildungskonzepte, die Bürgern und Verbrauchern helfen, sich auch beim Surfen im WWW und erst Recht bei finanziellen Transaktionen im Internet zu schützen. Für einen angemessenen Selbstdatenschutz ist also notwendig, daß sowohl verlässliche Informationen bereitgestellt als auch Technologien zum Schutz der persönlichen Daten entwickelt werden. Nur wenn das Wissen der Nutzer und die technischen Lösungen der Komplexität der Technik gerecht werden, können die Risiken wirksam minimiert werden.

Staatliche Datenschutz-Institutionen wie das ULD in Kiel, aber auch privatrechtliche Vereine und Verbände stellen diesbezüglich Informationen und Open-Source-Software zur Verfügung, so daß auch EDV-Laien sich selbst vor den Gefahren im Informationszeitalter effektiv schützen können.

Datensicherheit

Unter Datensicherheit wird die Bewahrung von Daten vor Beeinträchtigungen verstanden. Dabei zielt die Datensicherung besonders auf die Sicherstellung der Verfügbarkeit, der Integrität, der Verbindlichkeit und der Vertraulichkeit der Daten ab. Datensicherheit versteht sich als Datensicherung der sonstigen Daten (z.B. Konstruktionen, Forschungsergebnisse, Preise, usw).

Maßnahmen zur Datensicherheit umfassen unter Anderem physische/räumliche Sicherung der Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Maßnahmen der Datensicherung.

Datensicherheit ist eine Voraussetzung von Datenschutz. Nur wenn geeignete Schutzmaßnahmen getroffen werden, kann man davon ausgehen, daß vertrauliche bzw. personenbezogene Daten nicht in die Hände von Unbefugten gelangen.

In der Praxis handelt es sich bei einem effektiven Sicherheitskonzept um eine Kombination von technischen und organisatorischen Maßnahmen, bei denen insbesondere auch die beteiligten Menschen zielgerichtet (z.B. durch Weiterbildung) einbezogen werden.