Hauptseminar

Informatik und Gesellschaft

Prof. Dr. K. Lagally, S. Schimpf

Datenschutz im Zeitalter der Vernetzung

Martin Hetzinger

29. Mai 1997

Inhaltsverzeichnis

0.1 Einleitung

Die Vernetzung von Rechnern hat in den letzten Jahren stark zugenommen. Heute ist der isolierte Einzelrechner eher die Ausnahme. Firmen, Universitäten und Behörden haben ihre Computer nicht nur hausintern miteinander verbunden, sondern sind auch über das Internet in ein weltweites Netz eingebunden. Besonders durch Dienste wie Email oder WWW wurde das Internet auch bei privaten Nutzern populär – mittlerweile haben Millionen von Menschen einen Zugang und ein Ende des Wachstums ist noch nicht abzusehen.

Die Vernetzung von Rechnern vereinfacht den Austausch von Daten drastisch. Per Mausklick können in Sekundenschnelle weltweit Daten verschickt oder abgerufen werden. Damit, aber auch durch andere neue Informations- und Kommunikationstechniken, bekommt auch die Datenschutz-Problematik eine neue Dimension. Einige kritische Punkte sollen im folgenden aufgezeigt werden:

- **Dateibegriff**
  Die bestehenden Datenschutzgesetze gehen davon aus, daß es eine „speichernde Stelle“ gibt, die die Daten in einer Datei (manuell oder elektronisch) an einem Ort vorhält. Durch die Vernetzung lassen sich nun Daten auf mehrere Rechner an verschiedenen Orten verteilen. Der verwendete Dateibegriff trifft also nicht mehr in vollem Maße die Realität.

- **Chipkarten**
  Chipkarten erfreuen sich wachsender Beliebtheit. Sie vereinfachen viele alltägliche Vorgänge, wie Bankgeschäfte, Einkäufe oder Arztbesuche. Rechtlich ist dies allerdings schwierig einzuordnen: der Betroffene führt zwar seine Daten mit sich, hat also Verfügungsgewalt darüber, bei der Verwendung werden aber diese Daten mit Informationen aus anderen Quellen verknüpft (z.B. mit dem Kontostand aus dem Rechner einer Bank) und der Kunde hat darauf keinen Einfluß mehr. Momentan fehlen klare gesetzliche Bestimmungen für diesen Fall[1].

- **Übermittlung von Daten über Netz**
  Früher wurden Daten meist in Papierform übermittelt. Unbefugtem Zugriff beim Transport konnte man durch geschlossene Umschläge, in besonders wichtigen Fällen durch persönliches Überbringen, vorbeugen. Wenn Daten über das Internet verschickt werden, passieren diese unterwegs mehrere Knotenrechner. Auf jedem dieser Rechner kann eine Botschaft mitgehört, abgefangen oder verfälscht werden. Wer ist unter diesen Bedingungen für den Datenschutz beim Übermitteln verantwortlich?

- **Datenexport**
  Die weltweite Vernetzung von Rechnern macht das „Exportieren“ von Daten sehr einfach. Wer also deutsche Datenschutzgesetze umgehen will, kann die Daten ins Ausland übertragen und dort legal verarbeiten. Beispielsweise versuchte Opel Anfang der 80er Jahre, die Datenverarbeitung in die USA zu verlagern, was am Widerstand von Datenschutzbehörden scheiterte[2].

- **Nutzungs- und Kommunikationsprofile**
  Wer sich im Internet bewegt, tut das keineswegs anonym. Anbieter können die Aktivitäten der Nutzer verfolgen und so Kommunikationsprofile erstellen. Ein Anbieter im WWW beispielsweise kann feststellen, für welche Seiten sich ein „Surfer“ besonders interessiert und diesen (mindestens) mit Name

[1] siehe BfD: Tätigkeitsbericht [8], S. 406
[2] siehe Taeger [22], S. 11

und Email-Adresse identifizieren[3]. So läßt sich ein detaillierts Nutzerprofil erstellen, das sogar Auskunft gibt über persönliche Interessen oder politische Überzeugungen einer Person. Der Nutzer selbst merkt von alledem nichts. Von besonderem Interesse und wirtschaftlichem Wert sind solche Daten zum Beispiel für gezielte Werbung.

- **Nationale Regelungen - globale Netze**
  Das Internet ist ein weltweites Rechnernetz. Daten können einfach über Landesgrenzen hinweg ausgetauscht werden. Dazu kommt, daß dieses Netz niemandem gehört. Es gibt also keine zentrale Stelle die den Datenaustausch regulieren oder dafür verantwortlich gemacht werden könnte. Nationale Gesetze lassen sich unter diesen Bedingungen nicht durchsetzen. Dies gilt sowohl für die Inhalte die verbreitet werden (siehe Diskussion um Pornographie im Internet und den Versuch der deutschen Justiz, solche Inhalte sperren zu lassen), als auch für den Datenschutz.

Ein kleines Beispiel mag zeigen, welche juristischen Fragen auftreten können. Ein Stuttgarter, der Kunde eines amerikanischen Online-Dienstes ist, schickt seiner Bekannten, die an der Universität Stuttgart studiert, eine Nachricht per Email. Diese Mail wandert nun erst in die Zentrale des Providers in den USA, von dort über ein Gateway ins Internet, und über mehrere Knotenrechner, die in verschiedenen Ländern liegen können, zur Uni Stuttgart, wo sie schließlich der Studentin zugestellt wird. Dabei ist nun nicht einmal vorhersehbar, welche Rechner in welchen Ländern beteiligt sein werden. Innerhalb Deutschlands gilt das Brief- und Fernmeldegeheimnis und es gibt Datenschutzgesetze, aber wie sieht es in den anderen Ländern aus?

In den folgenden Kapiteln sollen nun die Datenschutzregelungen in Deutschland, in Europa und im internationalen Bereich betrachtet werden.

[3] Das *Center for Democracy and Technology* hat dazu unter
http://www.13x.com/cgi-bin/cdt/snoop.pl
eine *Privacy Demonstration Page* eingerichtet

Kapitel 1

Datenschutz in Deutschland

1.1 Gesetze zum Datenschutz – ein Überblick

1.1.1 Grundlagen des Datenschutzes

Grundlage des Datenschutzes ist das allgemeine Persönlichkeitsrecht, wie es im Grundgesetz verankert ist (Art. 1, Abs.1 Menschenwürde und Art. 2, Abs.1 freie Entfaltung der Persönlichkeit). Das Bundesverfassungsgericht hat dazu im sogenannten Volkszählungsurteil festgestellt: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[1]. Dieses informationelle Selbstbestimmungsrecht darf nur aufgrund einer verfassungsmäßigen gesetzlichen Grundlage und unter dem Grundsatz der Verhältnismäßigkeit eingeschränkt werden.

Wenn der Einzelne nicht überblicken kann, wer wann was über ihn weiß, kann er in seiner Freiheit, selbstbestimmt zu entscheiden oder zu handeln, wesentlich gehemmt werden. Dies würde nicht nur die individuelle Entfaltung des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, da Selbstbestimmung eine elementare Voraussetzung eines demokratischen Gemeinwesens ist.[2]

Für die Übermittlung von Daten, oder von Nachrichten ganz allgemein, gilt das Brief- und Fernmeldegeheimnis (GG Art.10, Abs.1). Es gilt auch für das Versenden von Nachrichten in elektronischer Form. Damit ist allerdings nur der Transport der Daten rechtlich gesichert.

1.1.2 Das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG, [1]) regelt den Umgang mit personenbezogenen Daten. Es legt im Einzelnen fest, unter welchen Voraussetzungen Daten erhoben, verarbeitet und genutzt werden dürfen. Das BDSG gilt für alle öffentlichen Stellen des Bundes und – mit Einschränkungen – für nicht-öffentliche Stellen (Private). Nicht-öffentliche Stellen sind natürliche oder juristische Personen des Privatrechts und Personenvereinigungen des Privatrechts. Dazu gehören unter anderem Einzelpersonen, Firmen und Vereine. Öffentliche Stellen der Länder haben sich nach den jeweiligen Landesdatenschutzgesetzen zu richten.

1.1.3 Bereichsspezifische Gesetze

Im BDSG sind allgemeine datenschutzrechtliche Prinzipen festgelegt. Darüber hinaus gibt es bereichsspezifische Regelungen, die den Datenschutz unter bestimmten

[1] Urteil BVerfGE 65, 1 vom 15.12.1983, Leitsatz 1
[2] Ebenda, Abschnitt C.II.

Bedingungen verschärfen oder einschränken. Beispiele hierfür sind das Steuergeheimnis oder das Personalaktengeheimnis einerseits, und Sonderbefugnisse von Polizei oder Verfassungsschutz andererseits. Folgende bereichsspezifische Gesetze sind im Zusammenhang mit der Vernetzung relevant:

- Das **Teledienstedatenschutzgesetz** (TDDSG) ist Teil des Informations- und Kommunikationsdienste-Gesetzes (IuKDG, [2]), das am 18.4.97 in den Bundestag eingebracht wurde. Es regelt unter anderem die Nutzung von Telediensten, die digitale Signatur und urheberrechtliche Fragen. Das TDDSG gilt für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung der Daten bestimmt sind und deren Übermittlung mittels Telekommunikation geschieht. Dazu zählen unter anderem Telebanking, Teleshopping, Informationsdienste, Internet-Dienste. Ob diese Angebote kommerziell oder unentgeltlich sind, spielt dabei keine Rolle.

- Das **Telekommunikationsgesetz** (TKG, [4]) reguliert in erster Linie den Wettbewerb in der Telekommunikationsbranche. Im Unterschied zum TDDSG geht es hier um Telekommunikationsdienstleistungen (also das Anbieten von Leitungen), nicht um die übermittelten Inhalte. Zu den Anforderungen, die ein Netzbetreiber erfüllen muß, gehören auch Datenschutzauflagen. Hier geht es vor allem darum, welche Daten der Betreiber über den Nutzer speichern darf, und wann er sie wieder löschen muß (§88).

  Sehr umstritten ist eine Regelung (§89), die vorsieht, daß der Anbieter der Regulierungsbehörde – und damit indirekt der Polizei, dem Verfassungsschutz etc. – eine Leitung zur Verfügung stellen muß, über die sie jederzeit Kundendaten abrufen kann. Kritiker sehen hier einen Schritt in Richtung Überwachungsstaat, da den Ermittlungsbehörden alle Informationen über das Kommunikationsverhalten der Bürger zur Verfügung stünden[3]. Es muß allerdings festgehalten werden, daß es hier um Kundendaten (Namen, Adressen, Telefonnummern, ...) geht und nicht um Verbindungsdaten[4]. Das Gesetz wurde am 25.7.1996 im Bundesrat verabschiedet.

1.2 Begriffe

In Datenschutzgesetzen tauchen immer wieder spezielle Begriffe auf. Ihre Bedeutung soll hier kurz erläutert und abgegrenzt werden:

- **Personenbezogene Daten:** Einzelangaben über persönliche Verhältnisse einer bestimmten oder bestimmbaren Person, z.B. Alter, Anschrift, Einkommen, Überzeugungen.

- **Datei:** Eine Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und sich nach bestimmten Merkmalen ordnen und auswerten läßt (manuell oder elektronisch).

- **Akte:** Sonstige, nicht in Dateiform vorliegende, Unterlage, die amtlichen oder geschäftlichen Zwecken dient.

- **Erheben:** Das Beschaffen von Daten.

- **Speichernde Stelle:** Jede Person oder Stelle, die Daten für sich selbst speichert oder im Auftrag speichern läßt.

[3] zur Kritik am TKG siehe [14] und [21]
[4] BfD: Tätigkeitsbericht [8], S. 182ff.

- **Verarbeiten:** Das Speichern, Verändern, Übermitteln, Sperren oder Löschen von Daten.
- **Nutzen:** Sonstige Verwendung von Daten (keine Verarbeitung), z.B. Ansehen auf dem Bildschirm.
- **Übermitteln:** Das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten. Die Daten werden dabei entweder von der speichernden Stelle weitergegeben oder vom Empfänger abgerufen.
- **Sperren:** Das Kennzeichnen gespeicherter Daten, um weitere Verarbeitung oder Nutzung einzuschränken.
- **Löschen:** Die Daten werden unkenntlich gemacht.
- **Bestandsdaten:** Daten die ein Dienstanbieter braucht, um das Vertragsverhältnis mit dem Kunden zu gestalten. Dazu gehören Angaben wie etwa die Anschrift des Kunden oder seine Kontonummer.
- **Verbindungs- und Nutzungsdaten:** Informationen über die Verbindungen, die ein Kunde herstellt und die teilweise zur Abrechnung benötigt werden. Beim Telefon sind dies Nummern und Uhrzeiten der geführten Gespräche. Im Internet die Information, welche Dienste genutzt wurden, also beispielsweise auch, an wen Emails verschickt wurden oder welche WWW-Seiten aufgerufen wurden.

1.3 Zulässiger Umgang mit Daten

Das Bundesdatenschutzgesetz unterscheidet an vielen Stellen zwischen der Datenverarbeitung in öffentlichen und in privaten Einrichtungen. Die Regelungen zur Erhebung, Speicherung und Übermittlung von Daten werden deshalb jeweils getrennt dargestellt.

1.3.1 Allgemeine Grundsätze

Generell gilt, daß die Verarbeitung von Daten nur zulässig ist, wenn dies ausdrücklich durch ein Gesetz erlaubt ist oder wenn der Betroffene dem zustimmt (BDSG §4, Abs.1 und TDDSG §3, Abs.1). Der Betroffene muß vorher über die Tragweite dieser Einwilligung unterrichtet werden. Die Einwilligung muß in der Regel schriftlich erfolgen. Der Nutzer eines Teledienstes kann sie auch in elektronischer Form abgeben, wenn sie durch eine eindeutige, bewußte Handlung des Nutzers erfolgt, die Urheberschaft klar ist und der Nutzer den Inhalt der Einwilligung jederzeit wieder abrufen kann (TDDSG §3 Abs.7).

1.3.2 Datenerhebung

a) Öffentliche Stellen

Es dürfen nur die Daten erhoben werden, die für die Erfüllung der Aufgabe erforderlich sind. Unnötige Datenansammlungen sollen vermieden werden. Die Daten müssen beim Betroffenen erhoben werden und ihm muß mitgeteilt werden, zu welchem Zweck das geschieht. In der Regel ist die Auskunft freiwillig; wenn nicht, so muß er über seine Rechte aufgekärt werden (BDSG §13). Ohne Mitwirkung des Betroffenen dürfen Daten nur in Ausnahmefällen und unter Beachtung entsprechender gesetzlicher Bestimmungen erhoben werden, etwa zur Abwehr von Gefahren durch die Polizei.

b) Privater Bereich

Hier werden personenbezogene Daten meist zu Geschäftszwecken verwendet. Die Daten müssen „nach Treu und Glauben" erhoben werden, das heißt unter freiwilliger Mitwirkung des Betroffenen. Heimlichkeit oder gar Nötigung sind verboten. Eine Firma darf also auch nicht Leistungen gegenüber dem Kunden von dessen Bereitschaft, Daten zur Verfügung zu stellen, abhängig machen (BDSG §28).

Teledienstanbieter müssen vor der Erhebung (auch wenn diese automatisch geschieht) den Nutzer über Art, Umfang, Zweck und Verarbeitung seiner Daten informieren. Sie dürfen Nutzungsdaten nur erheben, soweit dies notwendig ist, um dem Kunden die Nutzung der Dienste zu ermöglichen und hinterher abzurechnen. Sie sind sogar verpflichtet, ihre technischen Einrichtungen so zu gestalten, daß so wenig wie möglich personenbezogene Daten gespeichert werden (TDDSG §3, Abs.4, 5 und §6, Abs.1).

1.3.3 Speicherung, Veränderung und Nutzung

a) Öffentliche Stellen

Speicherung, Veränderung und Nutzung sind nur erlaubt, wenn dies für die Zwecke erfolgt, für die die Daten erhoben wurden. Diese Zweckbindung kann aufgehoben werden durch Gesetze, durch Zustimmung des Betroffenen oder wenn es offensichtlich im Interesse des Betroffenen liegt (BDSG §14).

b) Privater Bereich

Auch hier ist der Zweck der Maßstab. *Speicherung* und *Veränderung* sind erlaubt (BDSG §28),

- wenn ein Vertragsverhältnis (oder vertragsähnliches Vertrauensverhältnis) mit dem Betroffenen besteht (z.B. zwischen Bank und Bankkunde oder zwischen Arzt und Patient), zum Zweck der Vertragserfüllung,
- zur Wahrung berechtigter Interessen der speichernden Stelle,
- wenn die Daten aus allgemein zugänglichen Quellen (z.B. Telefonbüchern, Zeitschriften) entnommen werden können, oder wenn die speichernde Stelle sie selbst veröffentlichen dürfte,
- unter bestimmten Voraussetzungen zu Forschungszwecken.

Wenn erstmals personenbezogene Daten, die nicht allgemein zugänglich sind, für eigene Zwecke gespeichert werden, so muß der Betroffene davon unterrichtet werden. Werden die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert (Auskunfteien), dann muß die Benachrichtigung bei der ersten Übermittlung erfolgen (BDSG §33).

Die *Nutzung* ist auch erlaubt zur Wahrung berechtigter Interessen eines Dritten oder der Öffentlichkeit. Außerdem dürfen listenmäßig zusammengefaßte Daten über Angehörige einer Personengruppe genutzt werden, die sich beschränken auf

- Information über Zugehörigkeit zu der Gruppe,
- Berufsbezeichnung,
- Namen,
- akademische Grade,

- Anschrift und
- Geburtsjahr.

In allen Fällen gilt, daß Speicherung, Veränderung und Nutzung nur erlaubt sind, sofern nicht ein schutzwürdiges Interesse des Betroffenen überwiegt.

Teledienste dürfen Nutzerprofile nur bei Verwendung von Pseudonymen erstellen. Eine Zusammenführung des Nutzerprofils mit den Daten des Pseudonym-Trägers ist verboten (TDDSG §4, Abs.4).

1.3.4 Übermittlung von Daten

a) Öffentliche Stellen

Bei der Datenübermittlung unterscheidet das BDSG nach dem Empfänger. Ist dies eine andere *öffentliche Stelle*, so dürfen die Daten übermittelt werden, falls das zur Aufgabenerfüllung einer der Stellen notwendig ist. Das Zweckbindungsprinzip gilt aber auch hier: der Empfänger darf die Daten nur für den Zweck verwenden, für den sie erhoben wurden (BDSG §15).

Handelt es sich beim Empfänger um eine *nicht-öffentliche Stelle*, dann dürfen Daten übermittelt werden, wenn das zur Aufgabenerfüllung des Absenders erforderlich ist, oder wenn der Empfänger ein berechtigtes Interesse glaubhaft darlegen kann. Der Betroffene ist auf jeden Fall zu informieren. Für den Empfänger gilt eine strenge Zweckbindung. Die übermittelnde Stelle muß ihn ausdrücklich darauf hinweisen und jede Zweckänderung genehmigen (BDSG §16).

Werden schließlich Daten ins *Ausland* übermittelt, so gelten dieselben Grundsätze wie bei der Übermittlung an nicht-öffentliche Stellen. Auf keinen Fall dürfen Daten übermittelt werden, wenn Grund zu der Annahme besteht, daß damit gegen den Zweck eines deutschen Gesetzes verstoßen würde. Das wäre etwa der Fall, wenn politische Verfolgung im Empfängerland droht. Auch ausländische Empfänger müssen auf die Zweckbindung hingewiesen werden (BDSG §17).

b) Privater Bereich

Die Übermittlung personenbezogener Daten durch private Stellen ist dann erlaubt wenn auch eine Speicherung, Veränderung oder Nutzung zulässig ist (s.o. Abschnitt 1.3.3 b). Auch hier muß der Empfänger auf die Zweckbindung hingewiesen werden.

Widerspricht der Betroffene der Übermittlung seiner Daten für Werbezwecke, für Markt- oder Meinungsforschung, so ist diese unzulässig. Widerspricht er beim Empfänger, so muß der die Daten für diesen Zweck sperren (BDSG §28).

Die Werbewirtschaft unterhält eine Liste der Personen, die keine Werbesendungen wünschen. Jeder kann sich in diese „Robinson-Liste“ eintragen lassen. Antragsformulare gibt es unter folgender Anschrift:

Deutscher Direktmarketing Verband
– Robinson Liste –
Postfach 14 01
71243 Ditzingen
Tel. 07156/951010

Teledienstanbieter dürfen keine Nutzungs- oder Abrechnungsdaten ihrer Kunden an Dritte übermitteln. Ausnahme: anonymisierte Nutzungsdaten zu Zwecken der Marktforschung und Abrechnungsdaten, wenn dies zur Einziehung von Forderungen nötig ist (TDDSG §6, Abs.3).

1.3.5 Automatisches Abrufen von Daten

Richtet eine Stelle (öffentlich oder privat) ein Verfahren zum automatischen Abrufen von personenbezogenen Daten durch Dritte ein, so gilt Folgendes: ein solches Verfahren ist nur zulässig, wenn es den Geschäftszwecken bzw. Aufgaben der Stelle angemessen ist und schutzwürdige Interessen des Betroffenen berücksichtigt werden. Außerdem müssen der Zweck des Abrufverfahrens, die Datenempfänger, die Art der Daten und die Maßnahmen zur Gewährleistung des Datenschutzes schriftlich festgelegt werden (BDSG §10).

1.3.6 Datenverarbeitung im Auftrag

Wenn Daten im Auftrag durch andere Stellen verarbeitet werden, so ist der Auftraggeber für den Datenschutz verantwortlich (er hat ja auch die Daten erhoben). Der Auftrag muß schriftlich erteilt werden und die Art der Datenverarbeitung, sowie die technischen und organisatorischen Maßnahmen festlegen. Der Auftragnehmer darf die Daten nur auf Weisung des Auftraggebers nutzen (BDSG §11).

1.4 Rechte des Betroffenen

1.4.1 Auskunftsrecht

Grundsätzlich hat jeder das Recht zu erfahren, welche Daten über ihn gespeichert werden, woher diese Daten stammen und an wen sie weitergegeben wurden. Der Zweck der Speicherung und Personen oder Stellen, an die regelmäßig übermittelt wird, sind ebenfalls offenzulegen. Die Auskunft darf natürlich nur an den Betroffenen erteilt werden. Telefonische Auskünfte sind also nicht möglich, da der Anrufer nicht identifiziert werden kann. Im Normalfall darf die Auskunft nichts kosten. Ausnahme sind schriftliche Auskünfte, die sich wirtschaftlich nutzen lassen, etwa Bonitätsnachweise (BDSG §§19, 34).

Im Einzelnen unterscheiden sich die Regelungen für den öffentlichen und den privaten Bereich.

a) Öffentliche Stellen

Öffentliche Stellen des Bundes müssen ihre automatisierten Dateien dem Bundesbeauftragten in ein Register melden (s.u. Kapitel 1.5.1). Dieses Dateienregister darf von jedermann eingesehen werden. Hier sind allerdings nur Informationen über die Art – nicht den Inhalt – der gespeicherten Daten abgelegt (BDSG §26, Abs.5).

Personenbezogene Daten in Akten sind oft schwer auffindbar. Hier braucht die Auskunft nur gegeben zu werden, wenn der Betroffene Angaben macht, die das Auffinden ermöglichen und der Aufwand nicht außer Verhältnis zum Interesse des Betroffenen liegt (BDSG §19, Abs.1).

Die Auskunft über gespeicherte Daten wird verweigert, wenn sonst die Aufgabe der Stelle nicht ordnungsgemäß erfüllt werden kann (z.B. laufende polizeiliche Ermittlungen) oder wenn die Daten aus anderen Gründen geheimgehalten werden müssen (sehr selten, z.B. beim Adoptionsgeheimnis).

Ob Daten bei einem Nachrichtendienst (Verfassungsschutz, BND, MAD) gespeichert sind, darf nur mit Erlaubnis dieses Dienstes mitgeteilt werden (BDSG §19, Abs.3).

b) Privater Bereich

Stellen, die Daten geschäftsmäßig zum Zweck der Übermittlung speichern (z.B. Kreditauskunfteien) müssen auch Auskunft über Daten erteilen, die nicht in Dateien gespeichert sind. Wenn der Betroffene begründete Zweifel an der Richtigkeit der Daten hat, müssen sie auch mitteilen, woher sie ihre Daten haben und an wen sie weitergegeben wurden (BDSG §34, Abs.2).

Wenn für schriftliche Auskünfte Geld verlangt wird, muß dem Betroffenen die Möglichkeit gegeben werden, durch persönliche Einsicht kostenlos Auskunft über seine Daten zu erhalten. Auf diese Möglichkeit muß er ausdrücklich hingewiesen werden (BDSG §34, Abs.6).

Eine private Stelle darf die Auskunft nur verweigern, wenn keine gesetzliche Benachrichtigungspflicht besteht (BDSG §34, Abs.4). Die speichernde Stelle muß dann darlegen, aufgrund welcher gesetzlichen Bestimmung sie die Auskunft verweigert. Ist eine Auskunft unvollständig, so muß darauf hingewiesen werden.

1.4.2 Berichtigung, Löschung, Sperrung

Berichtigung

Jede speichernde Stelle ist verpflichtet unrichtige Daten zu korrigieren. Dazu muß natürlich auch der Betroffene beitragen, indem er auf falsche oder überholte Daten hinweist. In Akten werden falsche Daten nicht ersetzt, sondern durch einen Berichtigungsvermerk ergänzt (BDSG §§20, 35).

Löschung

Personenbezogene Daten müssen grundsätzlich gelöscht werden, wenn die Speicherung – und damit auch die vorangegangene Erhebung – unzulässig ist. Sie müssen auch gelöscht werden, sobald sie nicht mehr für den Zweck der Speicherung gebraucht werden (BDSG §§20, 35).

Für *nicht-öffentliche Stellen* besteht zusätzlich die Pflicht zum Löschen, wenn es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen oder politische oder religiöse Anschauungen handelt und deren Richtigkeit nicht bewiesen werden kann. Zum Zweck der Übermittlung gespeicherte Daten (Auskunfteien, Adressverlage) müssen fünf Jahre nach der ersten Speicherung überprüft und, wenn sie nicht mehr gebraucht werden, gelöscht werden (BDSG §35, Abs.2).

Teledienstanbieter müssen die Nutzungsdaten ihrer Kunden so früh wie möglich, spätestens nach Ende der jeweiligen Nutzung, löschen. Abrechnungsdaten müssen gelöscht werden, sobald sie zur Abrechnung nicht mehr erforderlich sind, bei Einzelnachweisen spätestens 80 Tage nach Versenden des Nachweises (TDDSG §6, Abs.2).

Sperrung

Gesperrt werden sollen Daten, wenn der Löschung besondere Gründe entgegenstehen. Dazu gehören Aufbewahrungsfristen, schutzwürdige Interessen des Betroffenen (wenn ihm etwa ein Beweismittel verlorenginge) und auch der Fall, daß die Löschung unverhältnismäßig aufwendig ist. Außerdem werden Daten gesperrt, wenn der Betroffene ihre Richtigkeit bestreitet und dieser Streit nicht geklärt werden kann (BDSG §§20, 35).

1.4.3 Anrufung von Kontrollinstanzen

Wer glaubt, daß er in seinen Rechten verletzt worden ist, kann sich an die jeweils zuständige Kontrollinstanz wenden. Für Behörden des Bundes ist dies der Bundesbeauftragte für den Datenschutz, für Einrichtungen der Länder die Landesdatenschutzbeauftragten und im nicht-öffentlichen Bereich die Aufsichtsbehörde des jeweiligen Landes, die entweder dem Landesbeauftragten oder dem Innenministerium unterstellt ist. Diese Stellen sind verpflichtet, allen Eingaben nachzugehen und den

Betroffenen vom Ergebnis zu unterrichten. Die Befugnisse dieser Kontrollinstanzen werden weiter unten in Abschnitt 1.5.3 näher beschrieben.

1.4.4 Schadensersatz

Speichernde Stellen sind zu Schadensersatz verpflichtet, wenn Daten unrichtig oder unzulässig verarbeitet werden. Diese Haftung geht noch über das Bürgerliche Gesetzbuch hinaus und soll so die Verantwortlichen zu besonders sorgfältigem Umgang mit personenbezogenen Daten anhalten.

Öffentliche Stellen haften, unabhängig von einem Verschulden, für Schäden bis 250.000 DM. Bei einer schweren Verletzung des Persönlickeitsrechts steht dem Betroffenen auch Schmerzensgeld zu (BDSG §7).

Für nicht-öffentliche Stellen gilt das Prinzip der Beweislastumkehr, das heißt die speichernde Stelle muß nachweisen, daß der entstandene Schaden nicht Folge eines von ihr zu vertretenden Umstandes ist. Wenn sie das nicht beweisen kann, haftet sie (BDSG §8).

1.5 Durchführung und Kontrolle

1.5.1 Dateienregister

Jede datenverarbeitende Stelle ist verpflichtet, alle für den Datenschutz wichtigen Informationen systematisch zu sammeln. Es muß ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen und ein Dateienregister geführt werden (BDSG §§18, 37). Diese Informationen sind wichtig, damit systematisch überprüft werden kann, ob alle Arbeitsabläufe den datenschutzrechtlichen Anforderungen genügen. Das Dateienregister enthält bei einer privaten Einrichtung folgende Informationen:

- Bezeichnung und Art der Dateien
- Art der gespeicherten Daten
- Geschäftszwecke, für die die Daten benötigt werden
- regelmäßige Datenempfänger
- Zugriffsberechtigungen von Personen oder Gruppen

Öffentliche Stellen müssen ganz ähnliche Dateienregister führen. Sie enthalten auch Regelfristen für die Datenlöschung. Stellen des Bundes müssen diese Informationen auch an den Bundesbeauftragten weiterleiten.

1.5.2 Technische und organisatorische Maßnahmen

Wie sollen nun Daten vor Mißbrauch und Verfälschung geschützt werden? Das BDSG macht dazu keine detaillierten Angaben. Es verlangt ganz allgemein „die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes ... zu gewährleisten“ (§9).

Für den Fall der automatisierten Datenverarbeitung legt eine Anlage zum Gesetz Mindestanforderungen fest. So muß sichergestellt werden, daß Unbefugten der Zugang zu den Datenverarbeitungsanlagen und zu den Datenträgern verwehrt bleibt (kein unerlaubtes Eingeben, Lesen, Verändern, Entfernen). Auch der Zugriff über Datenübertragungssysteme (Netz!) muß kontrolliert werden. Es müssen detaillierte Zugriffsberechtigungen installiert werden, so daß jeder nur die Daten anfassen kann, für die er eine Berechtigung hat. Außerdem muß überprüfbar sein, an welche Stellen Daten übermittelt werden können und wer wann welche Daten eingegeben hat.

Schließlich ist bei der Übermittlung die Sicherheit der Daten während des Transports zu gewährleisten.

Etwas konkreter äußert sich da der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der eine Orientierungshilfe zum Anschluß von Behörden an das Internet herausgegeben hat [15]. Er fordert, Verwaltungsnetze nur dann ans Internet anzuschließen, wenn dies unbedingt erforderlich ist und ein schlüssiges Sicherheitskonzept vorliegt. Die Einrichtung von Firewalls und der Einsatz von Verschlüsselung bei der Übermittlung sensitiver Daten wird gefordert.

Teledienstanbieter haben nach dem TDDSG noch besondere Pflichten. Sie müssen dem Kunden die Nutzung der Dienste und ihre Bezahlung anonym oder unter Pseudonym ermöglichen, wenn dies technisch möglich und zumutbar ist. Durch geeignete technische und organisatorische Maßnahmen muß außerdem sichergestellt werden, daß der Nutzer die Verbindung jederzeit abbrechen kann und daß die Daten über den Ablauf des Zugriffs sofort gelöscht werden (TDDSG §4, Abs.2).

1.5.3 Datenschutzbeauftragte

Notwendigkeit von Kontrollinstanzen

Jeder hat theoretisch die Möglichkeit, im Rahmen des Auskunftsrechts festzustellen, welche Daten über ihn im Umlauf sind und kann so die Einhaltung der Datenschutzgesetze kontrollieren. Trotzdem ist es notwendig und sinnvoll, besondere Kontrollinstanzen einzurichten, die die Umsetzung des Datenschutzes wirkungsvoll überwachen. Die Gründe liegen auf der Hand: die Kontrolle durch den Einzelnen ist begrenzt, denn der Aufwand ist immens und zumeist fehlt die juristische Sachkenntnis. In manchen Fällen, etwa bei den Sicherheitsbehörden, kann der Einzelne die Kontrolle gar nicht leisten. Hier wird sie stellvertretend von einem unabhängigen Kontrollorgan ausgeübt. Die für die verschiedenen Bereiche zuständigen Instanzen werden nun kurz vorgestellt.

Der Bundesdatenschutzbeauftragte

Der Bundesbeauftragte für den Datenschutz (BfD) wird vom Bundestag gewählt. Er ist weisungsunabhängig und nur dem Gesetz unterworfen. Seine Aufgaben sind die Beratung der Bundeseinrichtungen in Datenschutzfragen, die Kontrolle und die Bearbeitung von Eingaben. Kontrolliert werden alle öffentlichen Stellen des Bundes stichprobenartig. Die Bundesbehörden müssen ihm Fragen beantworten, Einsicht in Akten, Daten und Datenverarbeitungsprogramme gewähren und ihm Zutritt zu allen Diensträumen gestatten. Auch zu geheimen Daten muß ihm Zugang gewährt werden. Stellt der Bundesbeauftragte Verstöße fest, so beanstandet er diese und die höchste vorgesetzte Stelle (i.d.R ein Ministerium) muß sich darum kümmern. Alle zwei Jahre gibt er einen Tätigkeitsbericht heraus, in dem er über Kontrollmaßnahmen und Verstöße berichtet und aktuelle Probleme des Datenschutzes darstellt. Seine Anregungen wurden schon oft Anlaß, Gesetzesentwürfe zu ändern oder die Verwaltungsvorschriften datenschutzfreundlicher zu gestalten (BDSG §§22-26).

Die Landesdatenschutzbeauftragten

Die Länder haben entsprechend für den Bereich der Landes- und Kommunalbehörden einen Datenschutzbeauftragten. Er hat (zumindest in Baden-Württemberg) ähnliche Aufgaben und Befugnisse, wie der Bundesbeauftragte.

Aufsichtsbehörden der Länder

Für die Kontrolle im privaten Bereich sind die Aufsichtsbehörden der Länder zuständig. Diese sind normalerweise dem Innenministerium unterstellt, in machen Ländern übt auch der Landesbeauftragte diese Funktion aus. Sie überwachen die Einhaltung des Datenschutzes allerdings nur, soweit die Erhebung, Verarbeitung oder Nutzung in oder aus Dateien geschieht, oder wenn ein konkreter Verdacht auf einen Verstoß besteht. Die Aufsichtsbehörde hat dann das Recht, Geschäftsräume zu betreten, Unterlagen einzusehen und bei Mängeln Maßnahmen zur Abhilfe anzuordnen (BDSG §38).

Wer personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichert oder im Auftrag als Dienstleistungsunternehmen verarbeitet, muß seine Tätigkeit dieser Aufsichtsbehörde melden. Mitzuteilen sind Firmenname, Inhaber, Anschrift, Geschäftszwecke, Name des Datenschutzbeauftragten und Art der Daten (BDSG §32).

Für Teledienste gelten die Bestimmungen entsprechend. Hier kann die Behörde auch ohne einen konkreten Verdacht kontrollieren (TDDSG §8).

Betriebliche Datenschutzbeauftragte

Beschäftigt eine Firma ständig mehr als 5 Personen in der Datenverarbeitung, so muß sie eine fachkundige Person als Datenschutzbeauftragten einsetzen. Dieser ist auf dem Gebiet des Datenschutzes weisungsfrei und kann nur auf Verlangen der Aufsichtsbehörde abberufen werden. Er soll die Einhaltung der Vorschriften sicherstellen. Dazu gehört die Prüfung des Umgangs mit den Daten, der Datenverarbeitungsprogramme und die Schulung und Beratung des Personals in Datenschutzfragen (BDSG §§36, 37).

1.5.4 Strafrechtliche Bestimmungen

Verstöße gegen die wichtigsten Datenschutzvorschriften sind Straftaten und werden mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe belegt. Wer sich dabei zu bereichern oder einen Anderen zu schädigen versucht, kann sogar mit zwei Jahren Freiheitsentzug bestraft werden. Andere Verstöße sind Ordnungswidrigkeiten und werden mit Geldbußen bis zu 50.000 DM geahndet (BDSG §§43, 44).

Straftaten im Bereich des Datenschutzes werden allerdings nur auf Antrag des Betroffenen verfolgt.

Kapitel 2

Datenschutz in Europa

2.1 Konvention des Europarats

Der Europarat, eine 1949 gegründete internationale Organisation, hat zur Zeit 38 Mitgliedsstaaten. Dazu gehören neben den EU-Mitgliedern auch Staaten Osteuropas. Im Jahr 1981 hat der Europarat eine Konvention zum Datenschutz beschlossen, die 1985 in Kraft trat [7]. Inzwischen wurde die Konvention von 17 Staaten ratifiziert (Stand Ende 1996). Durch die Vereinbarung sollte der grenzüberschreitende Datenverkehr vereinfacht und gleichzeitig ein Mindeststandard für den Datenschutz geschaffen werden. Jeder Unterzeichnerstaat wurde verpflichtet, bis 1985 diesen Standard durch entsprechende nationale Gesetze umzusetzen. Dabei bleibt den Staaten allerdings eine gewisse Gestaltungsfreiheit.

Die festgelegten Grundsätze umfassen gesetzmäßige und faire Datenerhebung, die Bindung an den Zweck, für den die Daten erhoben wurden und das Prinzip der Verhältnismäßigkeit. Die Speichernde Stelle ist für die Sicherung der Daten verantwortlich. Dem Betroffenen werden Auskunfts- Berichtigungs- und Löschungsrechte zugesichert.

Für den Datenaustausch zwischen Mitgliedsländern wurde vereinbart, daß dieser nur unterbunden werden darf, wenn im Empfängerland für diese Art von Daten kein vergleichbarer Datenschutz existiert, oder wenn die Daten auf diesem Umweg in unsichere Drittstaaten gelangen können.

2.2 Richtlinie der EU

Der Rat der EU und das Europäische Parlament haben am 24.7.1995 eine Richtlinie zum Datenschutz [6] erlassen, die binnen 3 Jahren, also bis 1998, in nationale Gesetze umgesetzt werden muß. Die wesentlichen Abweichungen von der deutschen Gesetzgebung seien kurz dargestellt:

2.2.1 Anwendungsbereich

Ein wesentlicher Unterschied zum BDSG ist, daß die EU-Richtlinie nicht grundsätzlich zwischen öffentlichen und privaten Stellen unterscheidet. Trotzdem können nationale Gesetze eine solche Unterscheidung in einzelnen Punkten machen.

Die Richtlinie gilt für Verarbeitung personenbezogener Daten, die in Dateien gespeichert sind, oder die automatisch erfolgt (Art.3, Abs.1). Damit fallen unstrukturierte Akten nicht in den Geltungsbereich. Der Dateibegriff wird allerdings etwas weiter als im deutschen Recht gefaßt. Er umschließt auch dezentrale Datensammlungen (Art.2c). Damit sind auch verteilte Dateien gesetzlich erfaßt.

In den Erwägungsgründen der Richtlinie wird ausdrücklich darauf hingewiesen, daß die Bestimmungen auch für personenbezogene Ton- und Bilddaten gelten (Erwägungsgrund 14).

Nicht angewendet wird die Richtlinie auf Datenverarbeitung ausschließlich zu persönlichen oder familiären Tätigkeiten (Art.3, Abs.2).

2.2.2 Zulässiger Umgang mit Daten

Allgemeines

Auch in der EU gilt der Grundsatz, daß Daten nur erhoben und verarbeitet werden dürfen, wenn dies rechtmäßig und „auf Treu und Glauben" geschieht, der Zweckbindungs- und Erforderlichkeitsgrundsatz beachtet werden und die Richtigkeit und Aktualität der Daten sichergestellt wird (Art. 6).

Der für die Verarbeitung Verantwortliche kann sich der Regelungen nicht dadurch entziehen, daß er sich in einem Drittland niederläßt, denn in diesem Fall gilt das Recht des Staates, in dem sich die Datenverarbeitungsanlagen befinden (Erwägungsgrund 20).

Einzelentscheidungen, die nur aufgrund einer automatisierten Verarbeitung persönlicher Daten getroffen werden, sind unzulässig. Automatisierte Bewertungen der Kreditwürdigkeit oder der beruflichen Leistungsfähigkeit einer Person dürfen also nicht erfolgen (Art. 15). Hintergrund ist, daß Informationen in Dateien die Realität nur sehr verkürzt und unvollständig darstellen und so falsche Schlußfolgerungen zulassen. Aus den Kontobewegungen eines Kunden allein geht eben noch nicht hervor, was er sonst an Vermögen hat, was aber zur Bewertung der Kreditwürdigkeit von entscheidender Bedeutung ist. Dieser Artikel ist besonders relevant für den Bereich der Expertensysteme.

Datenübermittlung

Bei elektronischer Datenübermittlung ist der Absender, nicht der Netzbetreiber, für den Datenschutz verantwortlich. Wer also personenbezogene Daten per Email verschickt, muß sich auch um die Sicherung der Daten kümmern (Erwägungsgrund 47).

Die Übermittlung von Daten in *Drittländer* ist nur zulässig, wenn im Empfängerland ein angemessenes Datenschutzniveau gewährleistet ist. Die zuständige Kontrollbehörde (und im Zweifelsfall die EU-Kommission) entscheidet darüber, ob dies der Fall ist. Wenn in einem Drittland kein angemessener Datenschutz existiert, versucht die Kommission, durch Verhandlungen Abhilfe zu schaffen (Art. 25).

Ausnahmen sind Datenübermittlungen, denen der Betroffene zugestimmt hat, die im Rahmen eines Vertragsverhältnisses anfallen, oder die von lebenswichtigem Interesse für den Betroffenen sind (Art. 26).

2.2.3 Rechte des Betroffenen

Dem Betroffenen wird das Recht zugestanden, Auskunft über die zu seiner Person gespeicherten Daten zu erhalten, falsche oder unzulässige Daten verändern bzw. löschen zu lassen. Die speichernde Stelle muß im Fall einer Berichtigung, Sperrung oder Löschung auch Dritte, an die die Daten übertragen wurden, davon unterrichten (Art. 12). Außerdem kann der Betroffene gegen die Verarbeitung seiner Daten Widerspruch einlegen (Art. 14).

2.2.4 Durchführung und Kontrolle

Die für die Verarbeitung von Daten Verantwortlichen müssen ihre Aktivitäten einer Kontrollbehörde melden. Diese führt ein öffentliches Dateienregister. Die Meldepflicht kann nur aufgehoben werden, wenn die speichernde Stelle einen unabhängigen Datenschutzbeauftragten bestellt. Damit haben die Mitgliedsstaaten die Wahl, ob sie einen betrieblichen Beauftragten oder eine Meldepflicht installieren (Art. 18–19).

Die Mitgliedsstaaten müssen Kontrollinstanzen (wie etwa den Bundesbeauftragten) einrichten und mit entsprechenden Befugnissen ausstatten (Art. 28). Es wird auch auf europäischer Ebene eine Datenschutzgruppe mit Vertretern der Mitgliedsstaaten gebildet, die eine beratende Funktion hat (Art. 29–30).

2.2.5 Konsequenzen

Die einzelnen EU-Staaten müssen nun ihre Datenschutzgesetze dieser Richtlinie anpassen oder, wie Griechenland und Italien, solche Gesetze neu schaffen.

Schwachpunkte der EU-Richtlinie sind ihre zahlreichen Ausnahmebestimmungen, die letztendlich sehr verschiedene und damit auch vergleichsweise niedrige nationale Standards zuläßt. Aus Wirtschaftskreisen wird die Richtlinie zudem als zu bürokratisch kritisiert.

Im Rahmen der rechtlichen Harmonisierung steht nun auch eine Novellierung des BDSG an. Der Bundesbeauftragte sieht unter anderem in folgenden Punkten einen Reformbedarf des deutschen Gesetzes[1]:

- Die Aufsichtsbehörden der Länder sollen statt der Anlaßbefugnis eine umfassende Kontrollbefugnis erhalten.
- Es müssen (über die EU-Richtlinie hinaus) Regelungen für den Datenschutz bei Akten geschaffen werden.
- Die Verpflichtung der Betriebe, eigene Datenschutzbeauftragte zu benennen, macht die aufwendige und wenig erfolgreiche Meldepflicht überflüssig.
- Datenübermittlung in Drittländer muß geregelt werden.

[1] BfD: Tätigkeitsbericht [8], S. 404ff.

Kapitel 3

Datenschutz im internationalen Bereich

3.1 Die Datenschutzsituation

3.1.1 Mittel- und Osteuropa

Im Zuge ihres Wandels zu demokratischen Gesellschaftsformen erkennen diese Staaten zunehmend, wie wichtig der Schutz der Persönlichkeitsrechte für eine freiheitliche Gesellschaftsordnung ist. So sind in einigen dieser Staaten Datenschutzgesetze entworfen oder schon verabschiedet worden. Schwierigkeiten gibt es vor allem bei der Schaffung unabhängiger Kontrollinstanzen[1].

3.1.2 Andere Staaten

Besonders durch die Drittstaatenregelung in der EU-Richtlinie (s.o. Abschnitt 2.2.2) wurde die Aufmerksamkeit der Handelspartner der EU für Datenschutzfragen erregt. So bemühen sich inzwischen auch asiatische Staaten um ebenbürtige Datenschutzgesetze. Selbst in den USA ist man wach geworden, will aber das Problem durch Vereinbarungen mit der EU, statt mit verbesserten eigenen Regelungen lösen[2].

3.1.3 Internationale Organisationen

Neben dem Europarat (s.o. Abschnitt 2.1) gibt es weitere internationale Organisationen, die sich zum Datenschutz geäußert haben. Dazu gehört die OECD und auch die UNO. Es handelt sich allerdings nur um Leitlinien, nicht um bindende Vereinbarungen.

3.2 Das Internet – ein rechtsfreier Raum?

Bereits in der Einleitung wurde auf die rechtlichen Probleme weltweiter Rechnernetze hingewiesen: Wo ist das Internet? Welches Recht gilt? Wer entscheidet? Es geht hier nicht nur um Fragen des Datenschutzes. Im Bereich des Urheberrechts, des Lizenzrechts und des Strafrechts sieht es ganz ähnlich aus. Vor allem zu letzterem finden sich genügend Beispiele: von Kinderpornographie über nazistisches Gedankengut bis hin zur do-it-yourself-Anleitung für Bombenbastler und Hobbyterroristen

[1] BfD: Tätigkeitsbericht [8], S. 417ff.
[2] Ebenda, S. 419ff.

läßt sich fast alles übers Internet verbreiten, und wer sich geschickt dabei anstellt, entgeht der Strafverfolgung.

Das Internet gehört niemandem. Man kann es nicht einfach abschalten. Es gibt keine zentrale Person oder Organisation, die dafür verantwortlich ist. Folglich kann man auch Rechte nicht durchsetzen. Ist und bleibt das Internet also ein rechtsfreier Raum?

3.3 Mögliche Lösungen

Ein Ansatz besteht darin, zu hoffen, daß die – teilweise vorhandenen – Selbstregulierungsmechanismen im Internet genügen. Solche ungeschriebenen Gesetze beruhen auf freiwilliger Mitwirkung der Beteiligten. Wer dagegen verstößt, wird von der Netzgemeinschaft gerügt und im Extremfall ausgeschlossen. Man könnte auch allgemein anerkannte Schiedsstellen für Streitfälle einrichten. Damit kommt man aber vielen urheberrechtlichen und datenschutzrechtlichen Problemen nicht bei, weil hier die meisten Delikte still und unbemerkt geschehen.

Es gibt auch Überlegungen, das Internet als eigenständigen Rechtsraum aufzufassen. Es müßte dann eine eigene Gesetzgebung und Rechtssprechung geschaffen werden. Bedenken sind angebracht, weil der Konflikt dieses „Cyberlaw“ mit anderen, nationalen Rechtssystemen unausweichlich wäre.

Eine andere Lösung wäre, im Rahmen völkerrechtlicher Vereinbarungen weltweit verbindliche Regelungen zu finden. Wichtig wäre dann, daß möglichst *alle* Staaten der Welt sich daran beteiligen. Jede bestehende „Datenoase“ würde eine solche Vereinbarung untergraben. Einzelne Staaten könnten durch „Datendumping“ (im Sinne von besonders liberalen Gesetzen) die Datenverarbeitung an sich ziehen.

Außerdem setzt eine solche globale Zusammenarbeit voraus, daß ein Minimum an gemeinsamen Wertvorstellungen vorhanden ist. Dies ist bei Fragen des Datenschutzes oder der Meinungsfreiheit eher zweifelhaft[3].

Bleiben noch technische Vorkehrungen. Hier gibt es bereits eine Reihe von Verfahren, die zumindest einige der angesprochenen Probleme lösen können. Die Vertraulichkeit der Datenübermittlung kann mit Hilfe der Verschlüsselung gewährleistet werden. Der Gefahr der Identifikation im Netz kann durch Anonymisierung (z.B. bei Emails durch Remailer) begegnet werden. Auch für andere Rechtsbereiche gibt es solche Möglichkeiten (z.B. elektronische Wasserzeichen und Signaturen).

3.4 Fazit

Die Schwachpunkte der vorgeschlagenen Lösungen sind bereits genannt worden. Von den rechtlichen Maßnahmen hat wohl die Möglichkeit einer Vereinbarung im Rahmen der UNO über Mindeststandards eine gewisse Aussicht auf Erfolg, allerdings eher langfristig.

Bleibt zu hoffen, daß der Schub in Sachen Datenschutz, der durch die restriktive Drittstaatenregelung der EU ausgelöst wurde, dazu führt, daß die Datenschutzoasen im Laufe der Zeit weniger werden.

Noch ein Wort zu den technischen Maßnahmen: die Möglichkeit der Verschlüsselung ist die einzige Chance, die Vertraulichkeit der Kommunikation im Netz und damit auch ein Stück Datenschutz zu gewährleisten. Restriktive Gesetze oder gar Verbote der Verschlüsselung sind wenig hilfreich und wirken den Zielen des Datenschutzes entgegen.

[3] ausführlichere Erörterung der Lösungsansätze bei Mayer [18]

Literaturverzeichnis

[1] Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990,
BGBl. I S. 2954 (Stand August 1995)

[2] Informations- und Kommunikationsdienste-Gesetz (IuKDG) vom 18. April 1997
http://www.iid.de/rahmen/iukdg.html

[3] Entwurf der Begründung zum Referentenentwurf des IuKDG (Stand 28.06.1996)
http://userpage.fu-berlin.de/%7Emr94/epd/IuKDG-Begr.htm

[4] Telekommunikationsgesetz vom 25. Juli 1996,
BGBl. I S. 1120

[5] Gesetz zum Schutz personenbezogener Daten
(Landesdatenschutzgesetz - LDSG) vom 27. Mai 1991,
Gesetzblatt für Baden-Württemberg, 14. Juni 1991, S. 277ff.

[6] Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Datenschutz,
Amtsblatt der Europäischen Gemeinschaften Nr. L281 vom 23/11/95 S. 31

[7] Council of Europe, European Treaty Series No. 108, Signed January 28, 1981
http://www.rewi.hu-berlin.de/Datenschutz/International/
council_europe_data_protection_108_1981.txt

[8] Der Bundesbeauftragte für den Datenschutz: Tätigkeitsbericht 1995-1996
-16. Tätigkeitsbericht-, Bonn 1997

[9] BfD-INFO 1, Bundesdatenschutzgesetz -Text und Erläuterung-,
Bundesbeauftragter für den Datenschutz, Bonn 1996

[10] BfD-INFO2, Der Bürger und seine Daten,
Bundesbeauftragter für den Datenschutz, Bonn 1993

[11] BfD-INFO3, Schutz der Sozialdaten,
Bundesbeauftragter für den Datenschutz, Bonn 1994

[12] BfD-INFO4, Der behördliche Datenschutzbeauftragte,
Bundesbeauftragter für den Datenschutz, Bonn 1994

[13] Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997
http://www.bayern.de/DSB/DSBKEnt/TDKuDa.htm

[14] Presseerklärung des Landesbeauftragten für den Datenschutz Schleswig-Holstein vom 19.03.96
http://www.rewi.hu-berlin.de/Datenschutz/DSB/PE-SH-TKG.html

[15] Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet, 1.12.1995
http://www.hamburg.de/Behoerden/HmbDSB/Material/internet.htm

[16] „Budapest-Berlin Memorandum“, 20. Sitzung der Internat. Arbeitsgruppe für Datenschutz in der Telekommunikation, Berlin, 19.11.1996
http://www.datenschutz-berlin.de/diskus/13_19.htm

[17] Müller-Hengstenberg, Claus D.: Nationale und internationale Rechtsprobleme im Internet,
Neue Juristische Wochenschrift 28/1996, 10.7.96, S. 1777–1782

[18] Mayer, Franz C.: Recht und Cyberspace,
Neue Juristische Wochenschrift 28/1996, 10.7.96, S. 1782–1791

[19] Wuermling, Ulrich: Datenschutz bei Telediensten,
Datenschutz-Berater 12/1996, 16.12.96, S. 1–6

[20] Engel-Flechsig, Stefan: „Teledienstedatenschutz“,
Datenschutz und Datensicherheit 21 (1997), S. 8–16

[21] Ruhmann, Ingo: Der vollständige Artikel: Das neue Telekommunikationsgesetz,
DIE ZEIT 20/1996, 10.5.96

[22] Taeger, Jürgen: Grenzüberschreitender Datenverkehr und Datenschutz in Europa,
Papierflieger-Verlag, Clausthal-Zellerfeld 1995

[23] Dressel, Christian Oliver: Die gemeinsschaftsrechtliche Harmonisierung des europäischen Datenschutzrechts,
Verlag V. Florentz, München 1995

[24] Müller, G. F./Wächter, M.: Der Datenschutzbeauftragte,
Verlag C.H. Beck, München 1991

[25] Tinnefeld/Ehmann: Einführung in das Datenschutzrecht,
Oldenbourg Verlag, München 1992

[26] Tinnefeld/Philipps/Heil: Informationsgesellschaft und Rechtskultur in Europa,
Nomos-Verlag, Baden-Baden 1995