Informatik und Gesellschaft[1]

Notizen[2] zur „Vorlesung“[3] an der TU Dresden im SoSe 2010

Andreas Pfitzmann[4]

Ziele

Sensibilisierung für die durch den Einsatz von Informationstechnik und Informatikmethoden in der Gesellschaft bewirkten Änderungen, ihre Chancen und Risiken. Und auch anders herum: Identifikation der von der Gesellschaft ausgehenden Einflüsse auf Informationstechnik und Informatik.
Vermittlung von Argumentationsketten, Szenarien und empirischen Kenntnissen, kurzum: Reflexion und Denkanstöße, um eine individuelle persönliche Klärung von jetzigen Ausbildungs- und künftigen Arbeitszielen zu fördern. Dies soll eine bewusste und verantwortete Gestaltung informationstechnischer Systeme unterstützen.
Da mir bisher keine befriedigende Systematik für „Informatik und Gesellschaft“ bekannt ist, besteht die Vorlesung aus einer Sammlung breitgestreuter, jeweils separat verständlicher Themenmosaiksteinchen. Ihr/sein Gesamthemaverständnis muss jede(r) persönlich zusammensetzen.

Themenauswahl

Vorausschau: Informatik (computer science), Gesellschaft, und

Die prinzipielle Fehlerhaftigkeit
menschlichen Modellierens und Gestaltens,
physischer Geräte
sowie den planvollen Umgang mit dem Auftreten von Fehlern – Fehlertoleranz –

Verletzlichkeit der Informationsgesellschaft – innere und äußere Sicherheit

---

1 Offensichtlich ein echtes Teilgebiet von *Wissenschaft/Technik und Welt*.

2 Dies ist kein Skript, dafür ist es viel zu rudimentär und provisorisch! Es soll also mehr zum Denken anregen, als Gedachtes vermitteln. Wenn Sie Kritik oder Anregungen haben, dann kommen Sie bitte auf mich zu: Nöthnitzer Str. 46, Raum 3071, Institut für Systemarchitektur, Fakultät Informatik, TU Dresden, D 01062 Dresden, `http://dud.inf.tu-dresden.de/` Tel. 0351 / 463-38277, Fax 0351 / 463-38255, e-mail: pfitza@inf.tu-dresden.de

3 Oftmals sind Kritk und Anregungen auch für andere „HörerInnen“ der „Vorlesung“ interessant, hin und wieder möchte mensch etwas schriftlich diskutieren. Hierfür gibt es eine Mailingliste, auf die Sie sich unter **https://mailman.zih.tu-dresden.de/groups/listinfo/dud-iug** ein- und ggf. auch wieder austragen können.

4 Über so ein breites Thema wie I&G denkt mensch am besten nicht allein nach. Viele haben in den letzten 20 Jahren mit mir geredet, auf mich eingeredet, sich vermutlich auch über mein auf sie Einreden hin und wieder geärgert. Danke und Entschuldigung auch an all die, die ich hier nicht namentlich aufführen kann. Speziell für diese Notizen danke ich einerseits den HörerInnen der Vorlesung, die engagiert diskutiert und viele wichtige Anregungen gegeben haben. Andererseits haben Dr. Johann Bizer, Prof. Dr. Hannes Federrath, Dr. Michaela Huhn und Marit Hansen viel Engagement in die konstruktive Kritik von Teilen dieser Notizen und mancher meiner (An-)Sichten gesteckt. Nicht immer war ich einsichtig, so dass Fehler und Schwächen weiterhin allein mir zuzurechnen sind.

Rechnergestützte, integrierte Kommunikation
TKG: Das Ringen um Telekommunikationsüberwachung

soziale, kulturelle, politische und individuelle Auswirkungen der Informationstechnik und Informatik
Machtverschiebungen
informationelle (und kommunikative) Selbstbestimmung, Datenschutzrecht

Verantwortung, Berufsethos, Berufsethik, Berufsrecht, Hippokratischer Eid für InformatikerInnen?
gewerkschaftliche Berufsveränderung

EDV-Vertragsrecht bzw. allgemeiner Informationsrecht[5],

Grundlegende Urteile des Bundesverfassungsgerichts: Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung

Informatik und Menschenbild: Weder indeterministische Turingmaschine noch neuronales Netz?

Benimmregeln für Roboter?

Informatik und Arbeitswelt: Arbeitsplatzgestaltung (Ergonomie), Rationalisierung {Psychologie-Prof; Hannes Federrath fragen}

Informationstechnik als Umweltbelastung und -rettung

Open Source: Motive, Vorgehen und bisher Erreichtes

Informatik und 3. Welt {macht Dr. habil. Lazarek in einer eigenen Vorlesung}

Informatik und Behinderte

Geschlechtsspezifischer Umgang mit Informationstechnik ?

Verhaltensweisen in virtuellen Welten

Zukunftsdiskussion:
Was kommt von alleine?
Was würden wir uns wünschen?
Was können wir wie beeinflussen?

Lehr- und Lernformen

Gäste einladen, z.B. sächs. Datenschutzbeauftragten, Betriebsrat

Podiumsdiskussion, d.h. unterschiedliche Studies vertreten unterschiedliche Meinungen, bereiten Material vor, werten Diskussion aus[6]

Projekte und/oder Seminarvorträge an Studentengruppen (z.B. konträre Referate zum selben Thema) vergeben

Besichtigungen: Blindenkabinett

---

[5] Eine ausgezeichnete Einführung von Prof. Thomas Dreier: *Von Gütern, Kanälen und Speichern – Metaphern des Informationsrechts* im Umfang von 17 Seiten finden Sie unter **http://irafs1.ira.uka.de/~recht/deu/zar/veranst/dreier2001/Festrede.pdf** Zu einem Teil des Themas ein weiterer www-Tipp: „Ein Leitfaden zu ethischen und rechtlichen Fragen der Software-Nutzung“ `http://www.hrz.uni-dortmund.de/docs/Softwarenutzung.html`

[6] Ab SoSe 1996 gibt es Scheine nur noch für solche TeilnehmerInnen, die *aktiv* etwas in der oder für die Lehrveranstaltung getan haben.

Gliederung der Vorlesungsnotizen

Zum Vorlesungstitel

Informatik (computer science)

Wissenschaft von der systematischen Verarbeitung von Informationen, besonders der automatischen Verarbeitung mit Hilfe von Digitalrechnern. (aus dem Duden Informatik, BI, 1988, auch in vollst. überarbeiteter 2. Auflage, 1993)

Wissenschaft von der Informationsverarbeitung in Natur, Technik und Gesellschaft[7]. (Immo O. Kerner, 1994)

Je nach Perspektive wird Informatik eher als **Strukturwissenschaft**, wie die Mathematik[8], oder als **Ingenieurwissenschaft**, wie etwa Elektrotechnik und Maschinenbau[9], betrachtet.[10]

Gesellschaft (society)

Ganz als Laie gesagt: Die Chance oder der Alptraum, wie Menschen, in ihrer Basisfunktionalität also höhere Säugetiere, human hoffentlich mehr mit als gegeneinander leben können.

Ein paar *professionellere* Formulierungen:

Gesellschaft: zweckgebundene, aus Nützlichkeitserwägungen entstandene, meist in sich gegliederte Gruppe von Menschen, die zusammen leben und arbeiten.
aus: *Großes dt. Wörterbuch, 1973*

Gesellschaft [zu althochdt. giselliscaft „Vereinigung mehrerer Gefährten, freundschaftl. Beisammensein“], vieldeutig gebrauchter Begriff, der im weitesten Sinne die Verbundenheit von Lebewesen (Pflanzen, Tiere, Menschen) mit anderen ihrer Art und ihr Eingeschlossensein in den gleichen Lebenszusammenhang bezeichnet; allein auf den Menschen bezogen mein G. die *Menschheit* schlechthin oder bestimmte begrenzte Teile davon (z.B. die Menschen einer Nation) und weist auf deren Gliederung, [Rang]ordnung und bes. strukturiertes Beziehungssystem hin. ...

In bezug auf ihre Wirtschaftssysteme und polit.-staatl. Ordnungsverhältnisse unterscheidet man verschiedene **Gesellschaftssysteme** sowohl im Hinblick auf die geschichtl. Entwicklung der Menschheit (↑ Gesellschaftsformation) als auch auf die heute zu beobachtenden Unterschiede, wobei die Bez. für die verschiedenen G.systeme uneinheitlich ist und oft nur auf bestimmte Aspekte eines Systems bezogen ist (z.B. entwickelte bzw. Industrie-G., bürgerl. bzw. sozialist. G., Klassen-G. bzw. klassenlose G.). Jedes etablierte G.system besitzt ein relativ dauerhaftes inneres Gefüge (**Gesellschaftsstruktur** bzw. **Sozialstruktur**), das sich aus der Gesamtheit der gesellschaftl. Elemente (Individuen, Gruppen, Institutionen) zusammensetzt und durch deren sinnvolle Zuordnung und die damit verbundenen Normen, Handlungsmuster und Wertvorstellungen

---

7 Nach dieser sehr breiten Definition von Informatik wäre das Reflektieren über „Informatik und Gesellschaft“ Teil der Informatik. Zumindest heutzutage ist dies (leider) meistenteils nicht der Fall.

8 Dabei betrachtet die Mathematik eher statische, die Informatik eher dynamische Strukturen.

9 Duden Informatik, BI, vollst. überarbeiteter 2. Auflage, 1993, Seite 305: „Heute stellt sich die Informatik als eine Ingenieurwissenschaft dar, die (anstelle der Grundelemente 'Materie' und 'Energie') den Rohstoff 'Information' modelliert, aufbereitet, speichert, verarbeitet und einsetzt.“

10 Im SoSe 2007 meinte ein Hörer, Informatik unter Bezug auf „Informationsverarbeitung in Natur“ auch als Naturwissenschaft sehen zuwollen. Es fiel dann auch der Begriff „Neuronaturwissenschaft“, den Google noch nicht kennt.

gekennzeichnet ist. Von der *Soziologie* werden grundsätzlich die noch bei Naturvölkern zu beobachtende **genossenschaftl. Gesellschaftsform**, bei der zw. den verschiedenen Individuen und G.gruppen die Macht ausgewogen verteilt ist, und die **herrschaftl. Gesellschaftsform** unterschieden. Letztere zeichnet sich durch v.a. auf Grund gesellschaftl. Arbeitsteilung entstandene Ungleichheit der G.mitglieder sowie damit verbundene unterschiedl. Macht- bzw. Abhängigkeitsverteilungen aus und ist v.a. für die moderne Ind.gesellschaft kennzeichnend.

aus: *Meyers Grosses Taschenlexikon in 24 Bänden, BI, 4. vollst. überarb. Auflage, 1992*

Grundprobleme in einer Gesellschaft sind der **Interessenausgleich** zwischen ihren Mitgliedern bzw. verschiedenen Teilgruppen (wobei auch die zukünftigen Mitglieder der Gesellschaft sowie ggf. andere Gesellschaften zu berücksichtigen sind) sowie das Erreichen der gesamtgesellschaftlichen Ziele (sofern sie existieren). Der Interessenausgleich findet zwischen Einzelnen / Teilgruppen und der Gesellschaft als ganzes sowie ideellen Werten statt. Also

Interessenausgleich zwischen	Mitgliedern
	Einzelnen / Teilen / Gesamtgesellschaft
	Generationen
	Menschen / ideellen Werten (Zielen)

Der Interessenausgleich wird vor allem juristisch durch Gesetze und ihre gemeinschaftliche (≈ staatliche) Durchsetzung geregelt, ist ansonsten aber frei austragbar. Gesetze sollen jedem Menschen einen Satz Menschen- und Grundrechte (siehe Art. 1-19 GG) garantieren, sowie den „fairen“ Interessenausgleich sichern.

Der Interessenausgleich wird häufig nach ethischen Prinzipien beurteilt. Aus der Achtung der Würde des einzelnen Menschen werden

positive ethische Werte abgeleitet, z.B.

+ Gleichbehandlungsprinzip
+ Gerechtigkeit
+ Verantwortung
+ Solidarität
+ Friede

sowie negative ethische Werte, z.B.

- Egoismus
- Unbeherrschtheit
- Unehrlichkeit[11]

Für die Organisation des Interessenausgleichs und damit die Stabilität jeder Gesellschaft ist folgende **Grundtatsache aus der Psychologie** wichtig:

10% der Menschen sind immer ehrlich[12] und redlich[13].

---

[11] Bei geeigneten Definitionen der Begriffe sollte *Unehrlichkeit* nicht die Verallgemeinerung von *Höflichkeit* sein.

[12] Gemeint ist hier jeweils externe und nicht interne Ehrlichkeit, d.h. „ehrlich gegenüber anderen“ und nicht „ehrlich gegenüber sich selbst“.

[13] Insbesondere der Begriff „ehrlich“, aber auch der Begriff „redlich“ sind in gewisser Weise auf einer Meta-Ebene von „gut und böse“ angesiedelt. Insbesondere sind beide Begriffe orthogonal zu „richtig“, d.h. mensch kann sich auf ehrliche Weise falsch, auf unehrliche Weise richtig, auf unehrliche Weise falsch und – der Vollständigkeit halber – auch auf ehrliche Weise richtig verhalten. Meine Hoffnung ist, dass Verhaltensmaximen wie „ehrlich“ und „redlich“ in einer pluralistischen Gesellschaft eher konsensfähig sind als „gut und böse“ in allgemeiner und konkreter Form, also inkl. „richtig und falsch“.

80% der Menschen sind nur dann verlässlich ehrlich und redlich entgegen ihren Trieben und individuellen Vorteilen, wenn sie befürchten, dass unehrliches und unredliches Verhalten bekannt und bestraft wird.

10% sind immer latent unehrlich und unredlich.

Obige Zahlen sind natürlich ungenau, insbesondere da sie schwer zu ermitteln sind und sie natürlich von der genauen Bedeutung der Begriffe ehrlich/redlich abhängen.

Ebenso sollte versucht werden, Menschen durch charakterliche Bildung in Richtung höherer Ehrlichkeit und Redlichkeit zu beeinflussen. Leider waren solche Versuche in den letzten Jahrtausenden nicht gerade überwältigend erfolgreich.

Zusätzlich kann diskutiert werden, ob Menschen jeweils in eine Klasse gehören oder es adäquater ist, sie bzgl. unterschiedlicher Lebensbereiche (Politik, Beruf, Familie, etc.) oder Lebensabschnitte (Kindheit, Teeny, Erwachsener, etc.) möglicherweise unterschiedlichen Klassen zuzuordnen. Für die Schlussfolgerung, die ich aus obiger Grundtatsache ziehen möchte, sind diese Unterschiede glücklicherweise irrelevant.

Auch kann natürlich nicht erwartet werden, über die Ehrlichkeit und Redlichkeit eines Menschen zwischen unterschiedlichen Beurteilern Übereinstimmung zu erzielen.

Schließlich sei angemerkt, dass die mittlere Gruppe die für die Gesellschaftsbildung hauptsächlich relevante ist – und dies nicht nur ob ihrer Zahl, sondern auch wegen ihrer Prägbarkeit durch gesellschaftliche Konventionen und Zwänge.

Kurzum: Gesellschaft ist der manchmal in mancher Hinsicht gelingende Versuch, trotz Säugetiererbes und etlicher kulturell erlernter Zivilisationskriminalität (z.B. „Freie Fahrt für freie Bürger“) zumindest für einige Zeit in größeren Horden, vielleicht sogar als eine weltumspannende Horde, friedvoll miteinander zu leben. Hilfsmittel hierbei sind einerseits individuelle charakterliche Bildung und Ertüchtigung (Ethik, Religion, Toleranz, etc. – Sie haben da hoffentlich eigene Erfahrungen – manchmal hilft da sogar das Bildungssystem) und andererseits anerkannte und durchgesetzte Mechanismen zum Interessenausgleich und zur Konfliktbewältigung. Gesellschaft ist permanent von *innen* durch ihre eigenen Mitglieder bedroht, da es für Ehrlichkeit und Redlichkeit und damit wahrscheinlich auch für funktionierenden Interessenausgleich bei weitem keine stabile Mehrheit gibt. Seltener gibt es für eine Gesellschaft auch Bedrohungen von außen![14]

und (and)

hiervon handelt die „Vorlesung“.

Erste, grobe Beschreibungen dieses „und“ sind **gesellschaftsbezogene Charakterisierungen von Informatik** als

- Wissenschaft der rationalen, vorrangig maschinell unterstützten Verarbeitung von Informationen, die menschliche Fachkenntnisse und Kommunikation in technischen, ökonomischen und sozialen Bereichen unterstützen sollen (Übersetzung der Definition des Begriffs Informatique[15] der Académie Française nach [Coy_89 Seite 259]);
- sozial wirksame (Struktur-)Wissenschaft [Coy_89 Seite 256, 259];
- Wissenschaft des instrumentalen Gebrauchs der Informationstechnik [Coy_89 Seite 257];
- Wissenschaft von der Konstruktion neuer (manchmal zunächst nur virtueller) Realitäten;
- Wissenschaft der Maschinisierung der Kopfarbeit;

---

[14] Für eine Gesellschaft mag es mehrere *außen* und mehrere *innen* geben.

[15] L'Informatique: Science de traitment rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications, dans les domaines techniques, économiques et sociales.

- Rationalisierungswissenschaft [Coy_89 Seite 261];
- Gestaltungswissenschaft menschlichen, insbesondere gesellschaftlichen Zusammenlebens (Technikgestaltung hat tiefen Einfluß auf Arbeitsorganisation[16] und Freizeitgestaltung), also **Sozialingenieurswissenschaft**

Der Duden Informatik, BI, vollst. überarbeitete 2. Auflage, 1993, Seite 306f, umreißt **Informatik und Gesellschaft** folgendermaßen:

> „Ein relativ neuer Aspekt der Informatik, der sich zugleich mit dem großen Bereich der 'Technikfolgen-Abschätzung' auseinandersetzt, wird durch den Begriff *Informatik und Gesellschaft* ausgedrückt. Dieser Bereich behandelt die Auswirkungen der Informatik auf gesellschaftliche Entwicklungen: Ähnlich wie bei der Entwicklung mechanischer Maschinen (Schlüsselerfindung: Dampfmaschine, industrielle Revolution) wird auch der Computer als Instrument der ↑ Rationalisierung eingesetzt, woraus sich für die Betroffenen oft schwerwiegende soziale Folgen (Wandel von Arbeitsplätzen und beruflichen Anforderungen, ↑ Computer literacy) ergeben. In den letzten Jahren erkannte man auch zunehmend die Gefahren, die sich aus der schnellen Verfügbarkeit personenbezogener Daten und der Konzentration von Informationen in ↑ Datenbanken ergeben: Mögliche Einschränkung der Rechte des Einzelnen und Entstehung neuer Abhängigkeiten bzw. Machtverhältnisse durch die Verfügungsgewalt über Informationen (↑ Datenschutz). Schließlich kann der Computer zur Steuerung, Informationssammlung und -auswertung auf fast allen Gebieten von Wirtschaft, Wissenschaft, öffentlichem und privaten Leben eingesetzt werden und ermöglicht allein aufgrund seiner Arbeitsgeschwindigkeit die Lösung neuer, immer komplexerer Probleme. Entsprechende Computersysteme werden für den Menschen undurchschaubar, was zur Abhängigkeit von Spezialisten führt, Manipulationen Tür und Tor öffnet und die Situation jedes einzelnen nachhaltig in der Gesellschaft verändern kann.“

Kurz zusammengefasst:

> Informatik und Gesellschaft (Computers and Society) analysiert die Wechselwirkungen zwischen Informationstechnik sowie Informatik(methoden) und der Gesellschaft.

[16] „Aufgabe der Informatik ist also die Analyse von Arbeitsprozessen und ihre konstruktive, maschinelle Unterstützung. Nicht die Maschine, sondern die Organisation und Gestaltung von Arbeitsplätzen steht als wesentliche Aufgabe im Mittelpunkt der Informatik.“ [Coy_89 Seite 257]

Die prinzipielle Fehlerhaftigkeit

Fehlerhaftigkeit menschlichen Modellierens und Gestaltens

Modelle stellen prinzipiell nur einen *ungenau* abgebildeten *Ausschnitt* der Wirklichkeit dar.

—> Die Realität geht vor![17]

Modelle sind bestenfalls adäquat für einen *vorgegebenen Zweck* und durch den Menschen direkt (zumindest aber rechnergestützt) *handhabbar*.

Informatische Modelle ((Anwendungs-)Programme, ...) sind Teil der Wirklichkeit, wirken also auf sie ein und verändern damit oftmals ihren ihnen vorgegebenen Zweck. Informatische Modelle sind also, selbst wenn sie momentan adäquat sind, demnächst möglicherweise inadäquat.[18]

Modelle können, geschickt gewählt, als Welterklärungs- und damit Herrschaftsinstrument gebraucht werden, z.B. „Aufgrund der *biologischen* Abhängigkeit des Fötus von der Mutter und auch des Babys vom Stillen durch die Mutter, ist die Frau *natürlicherweise* für die Kinderaufzucht – und damit *zweckmäßigerweise* auch den ganzen sonstigen Haushalt – zuständig“.

—> Urteile über die Adäquatheit von Modellen dürften von den Interessen derjenigen abhängen, die sie beurteilen.

—> Modellbildung und -durchsetzung ist auch Machtausübung.

—> Zumindest angewandte Informatik, vermutlich auch Kerninformatik ist nicht interessen- und wertfrei!

—> Interessen und Werte sollten bewusst gemacht und explizit offengelegt werden (hoffentlich sorgen demokratische Prozesse dann nach und nach für global adäquat(er)e Modelle, z.B. sollten insbesondere Frauen ihr Wahl- und Welterklärungsrecht wahrnehmen).

Fehlerhaftigkeit physischer Geräte

Entwurfsfehler (Mensch, Werkzeuge, und beides rekursiv! —> transitive Trojanische Pferde)
Produktionsfehler
Alterungsbedingte Ausfälle
Sabotage
Elektromagnetischer Impuls (EMP = electromagnetic pulse), d.h. Atombombe in großer Höhe gezündet, zerstört alle elektronischen Geräte, die nicht sehr aufwendig „verbunkert“ sind, d.h. „Sichtverbindung“ zur Detonationsstelle haben

—> innerhalb von Millisekunden zurück in die Eisenzeit (Steinzeit wäre leicht übertrieben)!

Planvoller Umgang mit dem Auftreten von Fehlern

Fehlertoleranz, ja sogar Fehlerfreundlichkeit (Murphys law: If anything can go wrong, it will!)

Trau' keinem Menschen ganz (denn es gibt nur wenig charakterlich Verlässliche, die die notwendigen Fähigkeiten haben; beider Dinge müsste mensch sich sicher sein, um ganz vertrauen

---

[17] Sie mögen dies für trivial halten, es wird aber immer wieder ignoriert: 1998 ging durch die Massenmedien, dass ein Autofahrer, dem sein rechnergestütztes Navigationssystem eine Brücke über einen Fluss anzeigte, obwohl es nur eine Fähre gab, bei schlechter Sicht weiterfuhr. Da die Fähre ungeschickterweise gerade am anderen Ufer war, fand sich der Autofahrer wenig später mit seinem Auto im Fluss wieder.

[18] Dies kann auch als ein weiterer Aspekt von „ungenau“ beschrieben werden: Modelle sind nicht nur ungenau, weil sie notwendigerweise vergröbern, sondern sie können zusätzlich auch ungenau sein, weil sich die Wirklichkeit zwischen Modellbildung und Modellanwendung geändert hat.

zu können) und damit auch keinem Entwurf, Gerät, etc. ganz. Also ist für IT-Systeme grundsätzlich eine dezentrale Kontroll- und Implementierungsstruktur notwendig, vgl. mein Skript zu den Vorlesungen im Bereich Datensicherheit.

Verletzlichkeit der Informationsgesellschaft – innere und äußere Sicherheit

Literaturtipps: Alexander Roßnagel, Peter Wedde, Volker Hammer, Ulrich Pordesch: Die Verletzlichkeit der "Informationsgesellschaft"; Sozialverträgliche Technikgestaltung Vol. 5, Westdeutscher Verlag, Opladen 1989 (in der 2. Auflage von 1990 wurde nichts geändert).

Seite 1-5: Fiktive Story: Ausfall der Ortsvermittlungsstelle im Jahr 2019

Seite 73f: ***Neue Schadensverteilungen***:

Kumulationsschaden (... die neue Technik zu vielfachen, voneinander unabhängigen Handlungen verleitet – Missbrauchsmöglichkeiten von Systemen sprechen sich unter Interessierten schnell 'rum.)

Beispiele im Buch: viele Betrügereien an Geldausgabeautomaten; „Hacken“

Multiplikationsschaden (... durch die Technik multipliziert werden - viele brauchen / nutzen *dieselbe Technik* oder gar dasselbe System; extremes Beispiel: Sehr viele wichtige Dienste werden über *ein* diensteintegrierendes Kommunikationsnetz abgewickelt.)

Beispiel im Buch: Das Risiko, von einem Expertensystem eine falsche Antwort zu bekommen, mag nicht größer sein als bei der persönlichen Befragung eines Experten. Der Schaden kann sich jedoch multiplizieren, wenn ein Expertensystem von vielen Anwendern gleichzeitig genutzt wird.

Kopplungsschaden (... gleiche Schäden in scheinbar entkoppelten Systemen zum gleichen Zeitpunkt auftreten: physisch: EMP; logisch: Programmfehler bis hin zu Trojanischem Pferd oder gar transitivem Trojanischem Pferd.)[19]

Beispiel im Buch: Selbst entkoppelte und weitverteilte isolierte Systeme werden durch die gleiche Software/Firmware bzw. allgemeiner durch den gleichen Entwurf resultierend in der *gleichen Technik* sehr eng gekoppelt. Ein Fehler (oder eine Beeinflussung von Programmen) kann alle Nutzer gleichermaßen treffen. Enthält das Betriebssystem eines verbreiteten Rechners eine 'logische' Bombe, die dieses Programm zu einem bestimmten Zeitpunkt löscht, würden alle Anwendungen dieses Rechnertyps für unterschiedlichste Aufgaben mit einem Schlag ausfallen. Entsprechendes gilt bei Verwendung eines manipulierten Werkzeuges (Compiler, Editor, etc.) bzgl. der mit seiner Hilfe erzeugten Produkte.

hoher Einzelschaden. (... Schäden können besonders hoch werden, weil die neuen technischen Möglichkeiten bisherige Grenzen von Raum, Zeit, Energie oder Informationsdichte zu durchbrechen vermögen.)

Beispiele im Buch: Bereits das Versagen eines einzelnen IuK-Systems kann einen höheren Schaden verursachen, weil von ihm größere Wirkungen auf die Umwelt ausgehen, Teilschäden sich zu größeren Schäden entwickeln oder gestiegene Abhängigkeiten zu größeren Schadensfolgen führen.

Komplexschaden (Werden IT-Systeme miteinander vernetzt und sind sie von dieser Vernetzung abhängig, kann ein Technikausfall zu Schäden im gesamten Vernetzungskomplex führen.)[20]

---

[19] Der Unterschied zwischen Kumulationsschaden und Kopplungsschaden ist folgender: Bei *Kumulationsschäden* erfolgen *mehrere* autonome Willensentscheidungen von TäterInnen, die durch eine gemeinsam genutzte Sicherheitsschwäche motiviert sein können. *Kopplungsschäden* resultieren aus *einer* autonomen (Willens-)Entscheidung.

Beispiele im Buch: Ein Schaden in einem Servicerechenzentrum, in einer ISDN-Nebenstellenanlage oder gar im Telekommunikationsnetz wirkt sich sehr schnell auf alle angeschlossenen Teilnehmer aus.

Diese 5 IT-spezifischen Schadenstypen können jeweils für sich, aber auch vielfach vermischt vorkommen. Denkbar ist beispielsweise, dass die Kumulation von Schäden oder ein gemeinsamer Softwarefehler in Vermittlungsrechnern zum Ausfall eines Netzes und in der Folge zu vielen hohen Einzelschäden führt, vgl. Bild 1.

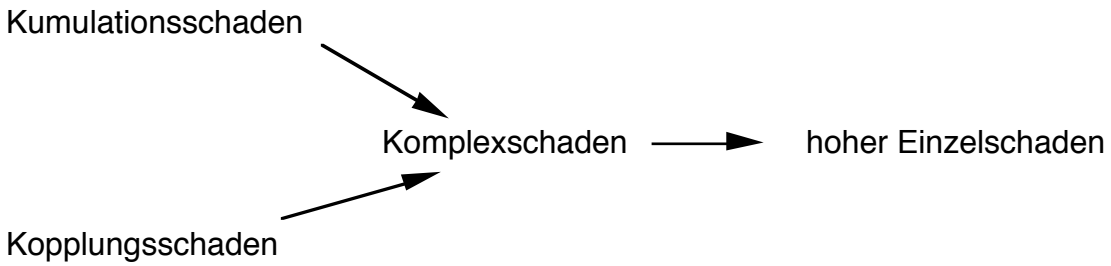


Bild 1: Ein Beispiel für das Zusammenwirken von Schadenstypen

Seite 208-213: ***Zehn Thesen zur Verletzlichkeit der Informationsgesellschaft***

1. Die Verletzlichkeit der Gesellschaft wird künftig ansteigen und zu einem zentralen Problem der 'Informationsgesellschaft' werden.
2. Die Struktur der Verletzlichkeit wird sich im Tatsächlichen wie im Wissen gegenüber heute verändern.
3. Das Sicherungsniveau könnte sehr hoch sein, wird in der Praxis aber deutlich unter den theoretischen Möglichkeiten liegen.
4. Die Sicherungssysteme werden sich sehr unterschiedlich entwickeln und immer wieder Lücken aufweisen.
5. Zahl und Intensität der Missbrauchsmotive nehmen überproportional zu.
6. Während die Erfolgswahrscheinlichkeit von Angriffen einzelner Externer erheblich reduziert werden kann, wird es keine ausreichende Sicherheit gegen Missbrauchsaktionen von Insidern geben. Insbesondere gegen die Angriffsformen des 21. Jahrhunderts sind keine zuverlässigen Sicherungen in Sicht. (Dies könnte als *Informatik-Kriminalität* bezeichnet werden.)
7. Komplexe IuK-Systeme sind nicht beherrschbar.
8. Das Schadenspotential von IuK-Systemen wird deutlich zunehmen. Die Gesellschaft wird in nahezu allen Bereichen vom richtigen Funktionieren dieser Technik-Systeme abhängig sein. Gesamtgesellschaftliche Katastrophen durch den Ausfall wichtiger sozialer Funktionen, die Techniksystemen übertragen wurden, sind nicht auszuschließen.
9. Sicherheit der IuK-Technik ist nur auf Kosten von Freiheit und Demokratie möglich, Freiheit und Demokratie können nur auf Kosten der Sicherheit erhalten werden.

---

[20] Vernetzung kann aber auch Redundanz und Entkopplung schaffen (Schutz *durch* verteilte Systeme, vgl. Skript zur Vorlesung Datensicherheit) und damit schadensmindernd wirken. Die Vervielfachung von Netzelementen erlaubt nämlich, beim Ausfall eines Netzknotens oder einer Übertragungsstrecke ohne Funktionsverlust auf andere umzuschalten. Werden Datenbestände und Datenverarbeitung dezentralisiert und von anderen entkoppelt, verteilt sich auch das Schadenspotential. Der Anschluss ans Netz erhöht die Chance, dass im Versagensfall ein anderes System die Funktionen des ausgefallenen übernehmen kann.

10. Die 'Informationsgesellschaft' setzt sich einem Sicherungszwang aus, den sie nicht mehr beherrschen kann und dessen Dynamik in sozialunverträgliche politische und soziale Verhältnisse zu führen droht.

These des Buches (aus meiner Sicht): Die künftige Informationsgesellschaft wird keine freundliche, tolerante, herrschaftsarme Gesellschaft sein, sondern das ungeheuere Schadenspotential der IT-Systeme erzwingt eine restriktiv gestaltete Überwachungsgesellschaft. Mindestens müssen die IT-Hersteller, -Produzenten und -Anwender vollständig überwacht werden.

Meine persönliche Einschätzung: Ohne außerordentliche Forschungs- und Entwicklungsanstrengungen im Bereich der Informatik und Informationstechnik stimmen die Thesen. Ich denke allerdings, dass IT-Systeme auch ohne Überwachungsstaat gegen Insider-Angriffe ausreichend gesichert werden können, vgl. mein Skript zu den Vorlesungen im Bereich Datensicherheit.

aktualisierender Literaturtipp: Ulrich Pordesch, Alexander Roßnagel: Untersuchungen zur Verletzlichkeit einer vernetzten Gesellschaft; in Raymund Werle, Christa Lang (Hrsg.): Modell Internet? Entwicklungsperspektiven neuer Kommunikationsnetze; Campus Verlag, Frankfurt/Main 1997, Seite 187-209 (abgedruckt im Anhang dieser Notizen).

Änderungen gegenüber 1989 (aus Sicht von 1997):

Umfassende Deregulierung, Liberalisierung und Privatisierung der Telekommunikation:

- definitiv kein Universalnetz einheitlicher Technik eines staatlichen Betreibers;
- demnächst mehrere Anschluß- und Verbindungsnetze unterschiedlicher privater Betreiber;
- demnächst auch Massenmarkt für satellitengestützte Mobilfunkempfänger;
- Telekommunikationsinfrastruktur vielfältiger {das ist vermutlich nur an der Oberfläche so, da die zugrundeliegenden Prozessoren und Betriebssysteme eher an Vielfalt verlieren – Schlagwort: Wintel}.

Netz-PCs (network PCs) könnten die technische Abhängigkeit von Netzen und die Risiken von Manipulationen und Ausforschungen steigern. Weitgehend autonome benutzerkontrollierte Endgeräte zu einer weniger verletzbaren Infrastruktur beitragen.

Internet: „Falschinformationen können von irgendwoher verbreitet werden, Angriffe auf Anwender können von jedem Winkel der Erde aus gestartet werden, ohne dass ein Betreiber oder Staat dies verhindern und oder auch nur den Verursacher erkennen und zur Rechenschaft ziehen kann.“ ... „Vieles scheint darauf hinzudeuten, dass die Risiken für die Verfügbarkeit“ der Telekommunikation „geringer werden, während Gefährdungen in bezug auf die Inhalte der Telekommunikation zunehmen.“ ... „auf technischer Ebene (bei den Servern und Endsystemen) aus Systemen weniger Hersteller besteht. Dadurch dürfte das Netz gegenüber bestimmten Manipulationen und physischen Attacken verwundbarer sein, als aufgrund des Vermittlungsprinzips gemeinhin angenommen wird.“

Stand 2010:

Während 1985 ISDN als Integrationstechnologie gesehen wurde, 1997 das Internet als Ergänzung zum Telefonnetz, wird **VoIP** (Voice over IP) 2005 zu einem Massendienst (vgl. u.a. Skype). Damit und durch die Ankündigung der Telekommunikationsfirmen (ca. auch 2005), ihre Kernnetze auf IP umzustellen, ist davon auszugehen, dass das **Internet die Integrationstechnik** wird, die den klassischen Fernsprechdienst obsolet macht – nicht aber das Fernsprechnetz im Teilnehmeranschlussbereich (dsl als die weitverbreitete Internet-Zugangstechnik benutzt die Telefonleitungen).

ergänzende Literaturtipps:

Volker Hammer: Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen; DuD-Fachbeiträge, Vieweg, Wiesbaden 1999.

Sushil Jajodia, Paul Ammann, Catherine D. McCollum: Surviving Information Warfare Attacks; Computer 32/4 (April 1999) 57-63.

Fred B. Schneider, Steven M. Bellowin: Evolving Telephone Networks; Communications of the ACM 41/1 (1999) 160.

National Research Council: Trust in Cyberspace; National Academy Press, 1999; `http://books.nap.edu/html/trust/index.htm`

Lauren Ruth Wiener: Digitales Verhängnis – Gefahren durch Computer und Software; Droemer, München 1996.

Prioritätsregelungen im juristischen Bereich

Um eine Einordnung von Gesetzen, Verordnungen, Richtlinien etc. (nennen wir sie kurz: juristische Regelungen) zu erleichtern, sei kurz dargelegt, welche(s) gilt, sollten welche miteinander im Konflikt stehen – wenn Sie so wollen, also eine Antwort auf die Frage:

Was ist die Prioritätenregelung im juristischen Bereich?

Ein Jurist würde die Frage etwas genauer formulieren:

Welche Rechtsquellen gelten wo und wann?

1. Jedes Gesetz, jede Verordnung, jede Richtlinie gilt nur in dem **geographischen Bereich**, für den das erlassende Organ zuständig ist – beispielsweise gelten deutsche Gesetze nicht in Frankreich.[21]
2. Juristische Regelungen, die **von übergeordneten Organen** erlassen werden, haben Priorität gegenüber Regelungen von untergeordneten Organen, beispielsweise gilt in der Bundesrepublik Deutschland: Verfassung[22] geht Gesetzen vor, d.h. verfassungswidrige Gesetze sind ungültig; Gesetze gehen Rechtsverordnungen vor, Rechtsverordnungen gehen Verwaltungsvorschriften vor[23]. Bundesrecht bricht Landesrecht, etc.. Dabei bezieht sich "übergeordnet" *auch auf den Gegenstandsbereich der Regelung*. Beispielsweise gibt es in der Bundesrepublik Deutschland eine Kulturhoheit der Bundesländer[24] – in diesem Bereich wäre der Bundestag also den Landesparlamenten nicht übergeordnet. Während innerhalb von Staaten normalerweise klar ist, welches Organ welchen anderen Organen in welchen Bereichen übergeordnet ist, ist dies im supranationalen Bereich manchmal unklar.
3. Bei juristischen Regelungen, die auf gleicher Stufe erlassen wurden (oftmals also vom gleichen Organ), gilt die **speziellere**. Beispielsweise gilt für den Umgang mit personenbezogenen Daten im Sozialbereich nicht das allgemeine Bundesdatenschutzgesetz (s.u.), sondern das speziellere Sozialgesetzbuch (SGB). *Oftmals ergibt sich dies auch aus den Gesetzen selbst*, z.B. §1 Bundesdatenschutzgesetz.
4. **Neuere** Regelung geht vor älterer Regelung.

Juristisch besonders kompliziert ist das im Verhältnis der Europäischen Union (EU) zu ihren Mitgliedsstaaten, vgl. Uwe Wesel: Europäische Einigung und staatliche Souveränität – wie verträgt sich das miteinander? Zum Beispiel bei der Rechtsprechung: Wer hat künftig das letzte Wort, das Bundesverfassungsgericht oder der Europäische Gerichtshof in Luxemburg? DIE ZEIT Nr. 15, 4. April 1997, Seite 44 und Constanze Stelzenmüller: Berufsverbot vor Gericht – Zwingen Europas Richter die Bundeswehr, Frauen an die Waffen zu lassen? DIE ZEIT Nr. 2, 5. Januar 2000, Seite 6.

Einerseits ist juristisch klar, dass EU-Gemeinschaftsrecht grundsätzlich Priorität gegenüber nationalen Recht, also auch nationalem Verfassungsrecht hat und damit der Europäische

---

[21] Es gibt, wie für fast alles im juristischen Bereich, Ausnahmen: Das deutsche Strafrecht (Strafgesetzbuch = StGB) gilt nicht nur in Deutschland, sondern auch für Deutsche im Ausland. Bei bestimmten gravierenden Straftaten gilt das StGB auch für Ausländer, die diese Taten im Ausland begangen haben.

[22] Die Verfassung der Bundesrepublik Deutschland heißt Grundgesetz (GG).

[23] Es gilt die Regel (Achtung: Unter Juristen heißt „Regel“ immer, es gibt auch Ausnahmen.): Gesetze beschließt das Parlament, Rechtsverordnungen beschließt die Regierung (Kabinett), Verwaltungsvorschriften erlässt der zuständige Minister.

[24] Solche Regelungen finden Sie im Grundgesetz.

Gerichtshof (EuGH) das letzte Wort hat. Andererseits hat sich das Bundesverfassungsgericht vorbehalten, EU-Gemeinschaftsrecht nicht anzuwenden, wenn es deutsche Grundrechte[25] in ihrem Wesensgehalt antastet. Für diese Fälle (die hoffentlich in der Praxis nie vorkommen) könnte das Bundesverfassungsgericht gegenüber dem EuGH das letzte Wort beanspruchen.

Zusätzlich ist für juristische Laien kompliziert, dass es auf der Ebene der EU Verordnungen und Richtlinien gibt. **EU-Verordnungen** (engl.: **Regulation**) sind in den Mitgliedsstaaten unmittelbar geltendes Recht, das bedeutet, sie gehen mitgliedsstaatlichen Gesetzen unmittelbar vor. **EU-Richtlinien** (engl.: **Directive**) hingegen sind nicht unmittelbar geltendes Recht, sondern verpflichten die Mitgliedsstaaten, innerhalb einer bestimmten Frist den Inhalt der EU-Richtlinie in mitgliedsstaatliches Recht umzusetzen. Verwirrend ist erst recht die Ausnahme, dass Richtlinien nach verstrichener Umsetzungsfrist unmittelbar die Mitgliedsstaaten binden, soweit ihr Inhalt ausreichend bestimmt ist.[26]

Neben der gerade erläuterten Unterscheidung von EU-Verordnung und EU-Richtlinie ist für den Laien besonders verwirrend, dass es auch in der Bundesrepublik (Rechts-)Verordnungen gibt. Diese sind aber nicht etwa Gesetzen vergleichbar (was die EU-Verordnungen ja sind), sondern den Gesetzen untergeordnet, etwa gibt es zu vielen Gesetzen in ihnen erwähnte (Rechts-)Verordnungen, die beispielsweise technische Details regeln – und natürlich nur insoweit gelten, als sie sowohl dem übergeordneten Gesetz nicht widersprechen als auch über den vom übergeordneten Gesetz gezogenen inhaltlichen Rahmen nicht hinausgehen.

Aufgabe

Denken Sie mal kurz darüber nach, welches Recht gelten könnte, wenn bei *e-commerce* ein Kunde in Land A bei einem Händler in Land B über einen Server in Land C eine Ware, z.B. ein Programm, kauft. Welches sind die Vor- und Nachteile der 3 Möglichkeiten? Welches Recht sollte Ihrer Meinung nach gelten?

Lösung

Sinnvollerweise gelten die Regelungen des Landes A oder B – lässt man C zu, dann könnte sich der Händler das Land, dessen Regelungen ihn am meisten begünstigen, nahezu beliebig aussuchen; außerdem ist es für den Kunden nahezu unmöglich festzustellen, wo der Server steht.

Gelten die Regelungen des Landes A (in der einschlägigen Diskussion **Bestimmungsland-prinzip** genannt), dann ist das sehr kundenfreundlich, denn der Kunde kennt seinen Rechtsraum. Schwierig ist das Bestimmungslandprinzip insbesondere für kleine Händler, die ihr Angebot auf solche Länder beschränken müssten, wo sie die Regelungen hinreichend kennen.

Gelten die Regelungen des Landes B (in der einschlägigen Diskussion **Herkunftslandprinzip** genannt), dann haben es zwar die Händler leicht, aber die Kunden müssten sich vor jedem Kauf fragen, ob sie die Regelungen von Land B hinreichend genau kennen. Das halte ich für noch weniger realistisch als dass die Händler eine Vielzahl von Regelungen kennen.

---

[25] Grundrechte sind nur ein kleiner, allerdings wichtiger Teil des Verfassungsrechts: Grundrechte geben Individuen stark garantierte, d.h. nicht oder zumindest nur schwer einschränkbare Freiheits- und Gleichheitsrechte, insbesondere gegenüber dem Staat.

[26] Es ist eine interessante Frage, welcher juristische Zustand dann zwischen Privatpersonen eintritt. Soweit ich weiß, gilt auch nach Ablauf der Frist die EU-Richtlinie für sie nicht unmittelbar. Allerdings hat wohl jede(r), dem aufgrund der fehlenden Umsetzung der EU-Richtlinie in mitgliedsstaatliches Recht ein Nachteil entsteht, einen Schadenersatzanspruch gegen den Mitgliedsstaat.

Datenschutzrecht

Prioritäten im Datenschutzrecht

Obige Prioritäten, angewandt auf das Datenschutzrecht, bedeuten nun:

1. Geographische Ordnung:
   - Die Europäische Datenschutzrichtlinie (EU-DatenschutzRL) gilt nur in der Europäischen Union.
   - Das Bundesdatenschutzgesetz (BDSG) gilt nur in Deutschland.
   - Das Sächsische Datenschutzgesetz (SächsDSG) gilt nur in Sachsen und zwar nur für den öffentlichen Bereich. Denn das Verhältnis von Bundes- und Landesgesetzgebung zueinander ergibt sich aus Art. 70 GG: Der Bund ist beispielsweise nach Art. 74 Nr. 11 für die Gesetzgebung für die Wirtschaft zuständig. Darunter fällt auch der Datenschutz in der Wirtschaft, folglich regelt der Bund im BDSG den Datenschutz nicht-öffentlicher Stellen.

2. Praktischerweise regeln die Regelungen des Datenschutzrechts regelmäßig ihren Anwendungsbereich in den ersten Paragraphen der betreffenden Regelung:
   - Die Europäische Datenschutzrichtlinie gilt nur, soweit die Regelungskompetenz der EU reicht (also beispielsweise nicht für die Datenverarbeitung durch die Polizei, Art. 3 Abs. 2 EU-DatenschutzRL).
   - Das BDSG gilt nur für die Datenverarbeitung öffentlicher Stellen des Bundes und nicht-öffentliche Stellen, weil der Bund nach dem GG nur insoweit die Regelungskompetenz besitzt (vgl. § 1 Abs. 2 BDSG).
   - Das SächsDSG gilt nur für die Datenverarbeitung der öffentlichen Stellen des Freistaates Sachsen.

3. Auch im Datenschutzrecht gilt der Grundsatz der bereichsspezifischen Regelung. Er findet sich zum Glück häufig auch in den Gesetzen selbst (vgl. § 1 Abs. 3 und 4 BDSG).
   - Für öffentliche Stellen, die Sozialdaten verarbeiten, gilt nicht das BDSG, sondern das SGB.
   - Für öffentliche Krankenhäuser die Datenschutzregelungen einzelner Landeskrankenhausgesetze der Länder. Für Ärzte speziell die Ärztliche Schweigepflicht der Berufsordnungen auf der Grundlage der Heilberufsgesetze der Länder und strafrechtlich (nur insoweit hat der Bund die Kompetenz) § 203 StGB.
   - Für Teledienste gilt das Teledienstedatenschutzgesetz, vgl. z.B. BfD-Info 5; Datenschutz in der Telekommunikation; 6. Auflage Februar 2004, kostenlos erhältlich beim BfD, siehe unten und digital unter `http://www.bfd.bund.de/information/pdf/info_5.pdf`.

4. Neuere Regelung gilt:
   - Für die Datenverarbeitung öffentlicher Stellen des Bundes und nicht-öffentliche Stellen in der Bundesrepublik Deutschland gilt nicht mehr das erste BDSG von 1977, oder das zweite vom 20.12.1990, sondern das „aktuelle“ BDSG vom 23.05.2001.

Das Bundesdatenschutzgesetz (BDSG)

Literaturempfehlungen:
BfD-Info 1; **Bundesdatenschutzgesetz** – Text und Erläuterung –; kostenlos erhältlich bei:
Der Bundesbeauftragte für den Datenschutz (BfD)
PF 200112, D-53121 Bonn, Fax 0228 / 819 9550, `http://www.bfd.bund.de/index.html`

Grundrecht auf Datenschutz ins Grundgesetz?
Hans-Hermann Schrader: Der Staat will zu viel wissen; Das Recht auf Datenschutz muss endlich ins Grundgesetz; DIE ZEIT /21 (20. Mai 1994) 14. {Datenschutz muss ins GG, damit Einschränkungen des Grundrechts auf Datenschutz im entsprechenden Gesetz explizit genannt werden müssen.}

Das Bundesdatenschutzgesetz (BDSG)

vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (BGBl. I, S. 2814)

(Hervorhebungen im Text von Andreas Pfitzmann, 15.04.2010)

Inhaltsübersicht

Erster Abschnitt
Allgemeine und gemeinsame Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) **Zweck** dieses Gesetzes ist es, **den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird**.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. **öffentliche Stellen des Bundes**,

2. **öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist** und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. **nicht-öffentliche Stellen**, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, **es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten**.

(3) Soweit **andere Rechtsvorschriften des Bundes** auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, **gehen** sie **den Vorschriften dieses Gesetzes vor**. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder

2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3 Weitere Begriffsbestimmungen

(1) **Personenbezogene Daten** sind **Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)**.

(2) **Automatisierte Verarbeitung** ist die **Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen**. Eine **nicht automatisierte Datei** ist jede nicht automatisierte **Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann**.

(3) **Erheben** ist das Beschaffen von Daten über den Betroffenen.

(4) **Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. **Speichern** das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,

2. **Verändern** das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. **Übermitteln** das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. **Sperren** das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. **Löschen** das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) **Nutzen** ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) **Anonymisieren** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) **Pseudonymisieren** ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) **Verantwortliche Stelle** ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) **Empfänger** ist jede Person oder Stelle, die Daten erhält. **Dritter** ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) **Besondere Arten personenbezogener Daten** sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) **Mobile personenbezogene Speicher- und Verarbeitungsmedien** sind Datenträger,

1. die an den Betroffenen ausgegeben werden,

2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(11) Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,

2. zu ihrer Berufsbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,

6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3a **Datenvermeidung** und **Datensparsamkeit**

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind **nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat**.

(2) Personenbezogene Daten sind **beim Betroffenen zu erheben**. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2.
   a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a **Einwilligung**

(1) Die Einwilligung ist **nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht**. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie **besonders hervorzuheben**.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,

2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder

3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30a nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

§ 4c Ausnahmen

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,

2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,

3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,

4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder

6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

§ 4d **Meldepflicht**

(1) Verfahren automatisierter Verarbeitungen sind **vor ihrer Inbetriebnahme** von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht **entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat**.

(3) Die Meldepflicht **entfällt** ferner, **wenn** die verantwortliche Stelle personenbezogene Daten **für eigene Zwecke** erhebt, verarbeitet oder nutzt, hierbei in der Regel **höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt** und entweder eine **Einwilligung** des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines **rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses** mit den Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen

geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung,

2. zum Zweck der anonymisierten Übermittlung oder

3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

(5) Soweit automatisierte Verarbeitungen **besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen**, unterliegen sie der Prüfung vor Beginn der Verarbeitung (**Vorabkontrolle**). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder

2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. **Name oder Firma** der verantwortlichen Stelle,

2. **Inhaber, Vorstände, Geschäftsführer** oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

3. **Anschrift** der verantwortlichen Stelle,

4. **Zweckbestimmungen** der Datenerhebung, -verarbeitung oder -nutzung,

5. eine Beschreibung der betroffenen **Personengruppen** und der diesbezüglichen Daten oder **Datenkategorien**,

6. **Empfänger** oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

7. **Regelfristen für die Löschung** der Daten,

8. eine **geplante Datenübermittlung in Drittstaaten**,

9. eine allgemeine **Beschreibung**, die es ermöglicht, vorläufig zu beurteilen, ob die **Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen** sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

§ 4f Beauftragter für den Datenschutz

(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten **automatisiert verarbeiten**, haben einen **Beauftragten für den Datenschutz schriftlich zu bestellen**. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der

Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten **nicht für die nicht-öffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen**. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum **Beauftragten für den Datenschutz** darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche **Fachkunde und Zuverlässigkeit** besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem **Leiter der** öffentlichen oder nicht öffentlichen **Stelle unmittelbar zu unterstellen**. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes **weisungsfrei**. Er **darf** wegen der Erfüllung seiner Aufgaben **nicht benachteiligt werden**. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs, bei nicht öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

(4) Der Beauftragte für den Datenschutz ist zur **Verschwiegenheit über die Identität des Betroffenen sowie über Umstände**, die Rückschlüsse auf den Betroffenen zulassen, **verpflichtet**, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben **erforderlich** ist, **Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel** zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den

jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

§ 5 **Datengeheimnis**

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 **Rechte des Betroffenen**

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf **Berichtigung**, **Löschung** oder **Sperrung** (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

(3) Personenbezogene Daten über die Ausübung eines Rechts des Betroffenen, das sich aus diesem Gesetz oder aus einer anderen Vorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten der verantwortlichen Stelle verwendet werden.

§ 6a Automatisierte Einzelentscheidung

(1) **Entscheidungen**, die für den Betroffenen eine **rechtliche Folge** nach sich ziehen **oder** ihn **erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden**, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(3) Das Recht des Betroffenen auf **Auskunft** nach den §§ 19 und 34 **erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten**.

§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (**Videoüberwachung**) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts oder

3. zur Wahrnehmung berechtigter Interessenfür konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 6c **Mobile personenbezogene Speicher- und Verarbeitungsmedien**

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,

2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,

3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und

4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 7 **Schadensersatz**

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles

gebotene Sorgfalt beachtet hat.

§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche **öffentliche Stelle** dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige **automatisierte** Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger **dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet**.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 9 **Technische und organisatorische Maßnahmen**

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die **erforderlich** sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn **ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht**.

§ 9a **Datenschutzaudit**

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und –programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,

2. Dritte, an die übermittelt wird,

3. Art der zu übermittelnden Daten,

4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden

getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundesoder Landesministerium zugestimmt hat.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der **Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich**. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf

hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1.
   a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4 f, 4 g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Zweiter Abschnitt
Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder

2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

§ 13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft vepflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,

2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,

3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,

7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,

8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder

9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. der Betroffene eingewilligt hat,

3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,

4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,

6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,

7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu

Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) **Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden**.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder

2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und

2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17 (weggefallen)

§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens, sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 19 **Auskunft** an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die **zu seiner Person gespeicherten Daten**, auch soweit sie sich auf die **Herkunft dieser Daten** beziehen,

2. die **Empfänger oder Kategorien von Empfängern**, an die die Daten weitergegeben werden, und

3. den **Zweck der Speicherung**.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund

gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,

2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die **Auskunft ist unentgeltlich**.

§ 19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder

3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 bis 4 gilt entsprechend.

§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass

personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(9) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21 Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 22 Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der **Deutsche Bundestag wählt auf Vorschlag der Bundesregierung** den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muss bei seiner Wahl das **35. Lebensjahr vollendet** haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

> "Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die **Amtszeit** des Bundesbeauftragten beträgt **fünf Jahre**. **Einmalige Wiederwahl ist zulässig**.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist **in Ausübung seines Amtes unabhängig** und nur dem Gesetz unterworfen. Er **untersteht der Rechtsaufsicht der Bundesregierung**.

(5) Der Bundesbeauftragte wird beim Bundesministerium des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,

2. mit der Entlassung.

Der Bundespräsident entlässt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Fall der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesministerium des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. Das Bundesministerium des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, **über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern**. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, dass über die

Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministeriums des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. **Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten**. Für den Bundesbeauftragten und seine Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, § 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der **Besoldungsgruppe B 9** zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§ 13 bis 20 und 21a Abs. 5 des Bundesministergesetzes mit der Maßgabe anzuwenden, dass an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren und an die Stelle der Besoldungsgruppe B 11 in § 21a Abs. 5 des Bundesministergesetzes die Besoldungsgruppe B 9 tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21 a Abs. 5 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.

(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs, und

2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in

Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Stellt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,

2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,

3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,

4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstattet dem Deutschen Bundestag **alle zwei Jahre einen Tätigkeitsbericht**. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 4 und 5 gilt entsprechend.

Dritter Abschnitt
Datenverarbeitung nicht-öffentlicher Stellen und öffentlichrechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht öffentliche Stellen,

2.
   a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   b) öffentlichen Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Bei

der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig:

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist
   a) zur Wahrung berechtigter Interessen eines Dritten oder
   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zunkunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt-

oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuchs genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 2 Nummer 2 Buchstabe b gilt entsprechend.

§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig:

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist
   a) zur Wahrung berechtigter Interessen eines Dritten oder
   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

   und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interessen an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass

die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nichtöffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 2 Nr. 2 Buchstabe b gilt entsprechend.

§ 28a Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4.
   a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
   b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,
   c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und
   d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

§ 28b Scoring

(1) Zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

2. im Falle der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für

eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,

4. im Falle der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und

2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Absatz 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

(1) Das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt.

Besondere Arten personenbezogener Daten (§ 3 Absatz 9) dürfen nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden.

(2) Für Zwecke der Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet oder genutzt werden. Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf, dürfen nur für das Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, wenn sie zuvor so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies nach dem Zweck des Forschungsvorhabens erforderlich ist.

(4) § 29 gilt nicht.

(5) § 28 Absatz 4 und 6 bis 9 gilt entsprechend.

§ 31 **Besondere Zweckbindung**

Personenbezogene Daten, die ausschließlich zu Zwecken der **Datenschutzkontrolle**, der

Datensicherung oder zur Sicherstellung eines **ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage** gespeichert werden, dürfen **nur für diese Zwecke verwendet** werden.

§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen

(1) **Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen**. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,

4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,

5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

7. die Daten für eigene Zwecke gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder
   b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

8. die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
   b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2)

und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,

9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) Im Fall des § 28 Abs. 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,

2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und

3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder

2. einen Bestandteil des Wahrscheinlichkeitswerts

berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Falle des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie

die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,

2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,

2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,

3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie

4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) **Die Auskunft ist unentgeltlich**. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene **einmal je Kalenderjahr** eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder

2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder unter nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) **Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen**. Er ist hierauf hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Fall des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zweck der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnis-

mäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt
Aufsichtsbehörde

§ 36 (weggefallen)

§ 37 (weggefallen)

§ 38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen**,** die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner

Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Vierter Abschnitt
Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,

2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,

3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42 Datenschutzbeauftragter der Deutschen Welle

(1) Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. Die §§ 4f und 4g bleiben unberührt.

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder

4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen

mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

Fünfter Abschnitt
Schlussvorschriften

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Marktoder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Sechster Abschnitt
Übergangsvorschriften

§ 45 Laufende Verwendungen

Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

§ 46 Weitergeltung von Begriffsbestimmungen

(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder

2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

§ 47 Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden

1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,

2. für Zwecke der Werbung bis zum 31. August 2012.

§ 48 Bericht der Bundesregierung

Die Bundesregierung berichtet dem Bundestag

1. bis zum 31. Dezember 2012 über die Auswirkungen der §§ 30a und 42a,

2. bis zum 31. Dezember 2014 über die Auswirkungen der Änderungen der §§ 28 und 29.

Sofern sich aus Sicht der Bundesregierung gesetzgeberische Maßnahmen empfehlen, soll der Bericht einen Vorschlag enthalten.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes

gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

8. zu gewährleisten, dass **zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet** werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Die EU-Datenschutzrichtlinie

Literaturempfehlungen:

Commission of the European Communities: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data; COM(92) 422 final – SYN 287, Brussels, 15 October 1992.

presented by the Commission pursuant to Article 149 (3) of the EEC Treaty;

1. Explanatory Memorandum: Main amendments: "The amended proposal ... drops the formal distinction between the rules applying in the public sector and the rules applying in the private sector. ... expands the provisions on the procedure for notification to the supervisory authority and on codes of conduct."

Verzeichnis der Änderungen; Synopse des alten und neuen Textvorschlages.

EG-Kommission: EG-Datenschutzrichtlinie; Geänderter Vorschlag der EG-Kommission vom 15.10.1992 für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr – COM(92) 422 final – SYN 287, Brussels, 15 October 1992; Datenschutz und Datensicherung DuD 16/12 (1992) 643-647.

Gemeinsame Stellungnahme der Obersten Aufsichtsbehörden der deutschen Länder für den Datenschutz im nicht-öffentlichen Bereich vom 08.02.1993: Zum Geänderten Vorschlag der Kommission der Europäischen Gemeinschaften vom 15.10.1992 für eine Richtlinie des Rates zum

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; Datenschutz und Datensicherung DuD 17/4 (1993) 227-232.

Ferdinand Kopp: EG-Datenschutzrichtlinie; Datenschutz-Berater 16/11 (1992) 1-7.

Zusammenfassende Erläuterung des geänderter Vorschlag vom 15. Oktober 1992 der EG-Kommission der EG-Datenschutzrichtlinie.

Stefan Walz: Zum Geänderten Vorschlag für die EG-Datenschutzrichtlinie vom 15.10.1992; Datenschutz und Datensicherung DuD 17/3 (1993) 134-135.

"Die Konkretisierung einer solchen Interessensabwägung erlaubt mithin eine erhebliche Bandbreite bereichsspezifischer Regelungen.".

Datenschutzrichtlinie der EU; Gemeinsamer Standpunkt des Rates der Europäischen Union vom 20.02.1995 im Hinblick auf den Erlass der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr; Datenschutz und Datensicherung DuD 19/4 (1995) 215-223.

Ulf Brühann: EU-Datenschutzrichtlinie – Umsetzung in einem vernetzten Europa; Datenschutz und Datensicherheit DuD 20/2 (1996) 66-72.

Ministerrat verabschiedete am 20. Februar 1995 Gemeinsamen Standpunkt zur EU-Datenschutzrichtlinie:

(vorbereitet von Arbeitsgruppe des Rates unter dem Vorsitz von Dr. Joachim Jacob)

nach [Kopp_95 Ferdinand Kopp: EU-Datenschutzrichtlinie: Gemeinsamer Standpunkt beschlossen; Datenschutz-Berater 19/3 (1995) 1-6]:

Für Europa **einheitlicher Datenschutzstandard**: Kein Mitgliedsstaat kann mehr den Datentransfer in einen anderen Mitgliedsstaat mit der Begründung verbieten, in dem anderen Mitgliedsstaat sei kein gleichwertiger Datenschutz gewährleistet.

Rahmen schaffen für die rasche und geordnete Entwicklung der neuen **Multimediatechnologien** (interaktives Fernsehen ermöglicht Persönlichkeitsprofile, wie es bisher selbst psychologische Tests nicht konnten; Funk- und Satellitentelefone ermöglichen Bewegungsprofile; automatische Gesundheitsbeobachter ...)

Richtlinie bietet notwendigen **Mindestschutz** und beschränkt sich auf **Prinzipien**. Wie beim BDSG **Verbot mit Erlaubnisvorbehalt**. Entsprechend der Europaratskonvention (vom 28. Januar 1981, enthalten im Anhang), auf der die Datenschutzrichtlinie aufbaut, werden gewisse Datenkategorien als besonders "sensibel" angesehen, z.B. rassische Zugehörigkeiten, politische oder religiöse Überzeugungen, Gesundheitsdaten und strafrechtliche Daten.

Die Richtlinie hat 4 Ansatzpunkte für Informationspflichten:

1. Datenerhebung,
2. Datenspeicherung- oder -weitergabe,
3. individuellen Auskunftsanspruch,
4. Einsicht in das öffentliche Datenverarbeitungsregister bei den Aufsichtsbehörden.

Mit dem Einbau der "betrieblichen Selbstkontrolle" in die Richtlinie konnten die ursprünglich vorgesehenen Meldepflichten noch weiter reduziert werden.

Viele Bestimmungen sind fakultativ, verpflichten die Mitgliedsstaaten also nicht, können aber in manchen Fällen als Empfehlung verstanden werden. Beispielsweise können die Mitgliedsstaaten

- das *Auskunftsrecht* der Betroffenen einschränken oder begrenzen, wenn dies zum Schutz der nationalen Sicherheit oder der Landesverteidigung erforderlich ist oder
- statt der *Gefährdungshaftung* für Schäden, die der Verarbeiter verursacht hat, ganz oder teilweise eine *Verschuldenshaftung* vorsehen.

Als nächstes muss nun innerhalb von 4 Monaten das Europäische Parlament die Datenschutzrichtlinie annehmen oder abermals Änderungsvorschläge machen.

Europäisches Parlament hat am 15. Juni 1995 Gemeinsamen Standpunkt zur EU-Datenschutzrichtlinie mit sieben Änderungen angenommen

Sowohl die Kommission als auch der Rat der Europäischen Union (am 24. Juli 1995) haben die Änderungswünsche akzeptiert. Damit ist die folgende Fassung der Datenschutzrichtlinie endgültig beschlossen. Die Mitgliedsstaaten müssen die Datenschutzrichtlinie nun innerhalb von 3 Jahren in nationales Recht umsetzen – also bis zum 24. Juli 1998. Das ist in der Bundesrepublik bzgl. des BDSG nicht rechtzeitig geschehen. Der aktuelle Entwurf des BDSG vom 06.07.1999 ist unter `http://www.dud.de` Aktuelles zu finden.

nach [Datenschutzrichtlinie der EU – endgültig! Datenschutz und Datensicherheit 19/8 (1995) 483]:

Größtenteils wörtliche Auszüge: Datenschutzrichtlinie der EU

vom 24.07.1995 – Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr[27].

§1 Gegenstand der Richtlinie

1. Die Mitgliedsstaaten gewährleisten ... den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.
2. ... freien Verkehr personenbezogener Daten zwischen den Mitgliedsstaaten ...

§ 2 Begriffsbestimmungen

a) personenbezogene Daten: alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“)

d) Verantwortlicher der Verarbeitung: die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. ...

§ 3 Anwendungsbereich

1. ... ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in Dateien gespeichert sind oder gespeichert werden sollen.
2. ... findet keine Anwendung auf die Verarbeitung personenbezogener Daten,
   - die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen ... die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

[27] abgedruckt in DuD, Datenschutz und Datensicherung, Vieweg 19/4 (1995) 215-223 und 19/8 (1995) 483.

- die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.

§ 6 Grundsätze in Bezug auf die Qualität der Daten

a) Verarbeitung ... nach Treu und Glauben und auf rechtmäßige Art und Weise.
b) Zweckbestimmung bei Erhebung (Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorangegangenen Datenerhebung anzusehen, sofern die Mitgliedsstaaten geeignete Garantien vorsehen)
c) Daten müssen den Zwecken entsprechen, dafür erheblich sein und nicht darüber hinausgehen.
d) Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit... nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden.
e) die Daten dürfen nicht länger in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht, als für die Realisierung der angestrebten Zwecke erforderlich

§7 Grundsätze in bezug auf die Zulässigkeit der Verarbeitung von Daten

Die Mitgliedsstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;
b) die Verarbeitung ist erforderlich für die Erfüllung des Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;
c) ... rechtlichen Verpflichtung ...
d) ... erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
e) ... erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt ...
f) ... erforderlich zur Verwirklichung des berechtigten Interesses, das von dem Verantwortlichen der Verarbeitung oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß § 1 Absatz 1 geschützt sind, überwiegen.

§8 Verarbeitung besonderer Kategorien personenbezogener Daten

1. Die Mitgliedsstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.
2. Absatz 1 findet in folgenden Fällen keine Anwendung:
   a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden; oder
   b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des Verantwortlichen der Verarbeitung auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, ...
   c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, ...
   d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer berechtigten Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder

der Organisation ... bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder

e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

...

7. Die Mitgliedsstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.

§ 10 Informationen bei der Erhebung personenbezogener Daten bei der betroffenen Person

... die Person, bei der die sie betreffenden Daten erhoben werden, ... zumindest die nachstehenden Informationen erhält ...

a) Identität des Verantwortlichen der Verarbeitung ...
b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind,
c) weitere Informationen, beispielsweise betreffend
   - die Empfänger oder Kategorien der Empfänger der Daten,
   - die Frage, ob die Beantwortung der Fragen verpflichtend oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung,
   - das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

   sofern sie ... notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

§ 12 Auskunftsrecht

Die Mitgliedsstaaten garantieren jeder betroffenen Person das Recht, vom Verantwortlichen der Verarbeitung folgendes zu erhalten:

1. frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten
   - die Bestätigung, dass es Verarbeitung sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden;
   - eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;
   - Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, ...
2. je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;
3. die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Nummer 2 durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

§ 15 Automatisierte Einzelentscheidungen

1. Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

§ 16 Vertraulichkeit der Verarbeitung

... personenbezogene Daten nur auf Weisung des Verantwortlichen der Verarbeitung verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.

§ 17 Sicherheit der Verarbeitung

1. ... der Verantwortliche der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.
   Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

§ 18 Pflicht zur Meldung bei der Kontrollstelle

1. ... Meldung des Verantwortlichen der Verarbeitung ... bei der in § 28 genannten Kontrollstelle vor, ...
2. ... Vereinfachung oder ein Entfallen der Meldung nur in den folgenden Fällen ...
   - ... für Verarbeitungskategorien, bei denen unter Berücksichtigung der verarbeiteten Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, ...
   - der Verantwortliche der Verarbeitung bestellt entsprechend dem einzelstaatlichen Recht, dem er unterliegt, einen Datenschutzbeauftragten ...

§ 20 Vorabkontrolle

1. Die Mitgliedsstaaten legen fest, welche Verarbeitungen geeignet sind, spezifische Risiken für die Rechte und Freiheiten der Personen aufzuweisen, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.
2. Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung ... vor, oder sie erfolgen durch den Datenschutzbeauftragten, der im Zweifelsfall die Kontrollstelle konsultieren muss.

§ 21 Öffentlichkeit der Verarbeitung

1. Die Mitgliedsstaaten erlassen Maßnahmen, mit denen die Öffentlichkeit der Verarbeitungen sichergestellt wird.
2. Die Mitgliedsstaaten sehen vor, dass die Kontrollstelle ein Register der gemäß § 18 gemeldeten Verarbeitungen führt.

§ 23 Haftung

1. Die Mitgliedsstaaten sehen vor, dass jede Person, der ... ein Schaden entsteht, das Recht hat, von dem Verantwortlichen der Verarbeitung Schadenersatz zu verlangen.
2. Der Verantwortliche der Verarbeitung kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.

§ 25 Übermittlung personenbezogener Daten in Drittländer; Grundsätze

1. ... Übermittlung ... in ein Drittland ... zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

§ 28 Kontrollstelle

1. Die Mitgliedsstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedsstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.
   Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.
2. Die Mitgliedsstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Verwaltungsmaßnahmen oder -vorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.
3. Jede Kontrollstelle verfügt insbesondere über
   - Untersuchungsbefugnisse ...
   - wirksame Einwirkungsbefugnisse ...
   - das Klagerecht oder eine Anzeigebefugnis ...
4. Jede Person oder ein sie vertretender Verband kann sich ... an jede Kontrollstelle mit einer Eingabe wenden. ...
5. Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

...

7. Die Mitgliedsstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

§ 29 Datenschutzgruppe (auf EU-Ebene)

1. ... ist unabhängig und hat beratende Funktion ...

§ 30 (Aufgabe der Datenschutzgruppe)

1. ... hat die Aufgabe,
   a) alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;

...

6. ... erstellt jährlich einen Bericht ... wird veröffentlicht.

§ 32 (Übergangsbestimmungen)

1. Die Mitgliedsstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen. ...[28]

§ 33 (Begleitung durch Kommission der EU)

1. Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig ... einen Bericht über die Durchführung dieser Richtlinie vor und fügt ihm gegebenenfalls geeignete Änderungsvorschläge bei. Dieser Bericht wird veröffentlicht.
2. Die Kommission prüft insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung personenbezogener Bild- und Tondaten und unterbreitet geeignete Vorschläge, die sich unter

---

[28] Diese Frist endete am 24.10.1998. Innerhalb der Bundesrepublik Deutschland hatte zu diesem Termin lediglich Hessen sein Datenschutzgesetz angepaßt. Inwieweit ansonsten die EU-Datenschutzrichtlinie unmittelbar gilt, wird in Christian Haslach: Unmittelbare Anwendung der EG-Datenschutzrichtlinie; DuD, Datenschutz und Datensicherheit 22/12 (1998) 693-699 eingehend erörtert.

Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten.

Vergleich

BDSG (vom 20.12.1990)	**Datenschutzrichtlinie der EU** (vom 24.07.1995)	**BDSG** (vom 20.12.1990, geändert am 23.05.2001, 29.07.2009 und 14.08.2009)
Unterscheidung öffentlicher Bereich (2. Abschnitt) nichtöffentlicher Bereich (3. Abschnitt)	keine Unterscheidung	Unterscheidung öffentlicher Bereich (2. Abschnitt) nichtöffentlicher Bereich und öffentlich-rechtliche Wettbewerbsunternehmen (3. Abschnitt)
Verbot mit Erlaubnisvorbehalt (§4)	Verbot mit Erlaubnisvorbehalt (§7)	Verbot mit Erlaubnisvorbehalt (§4)
Auskunft grundsätzlich unentgeltlich (§19 (7))	Auskunft ohne übermäßige Kosten (§12)	Auskunft grundsätzlich unentgeltlich (§19 (7))
Datenschutzbeauftragte in nicht-öffentlichen Stellen, die personenbezogene Daten verarbeiten, sind obligatorisch (§36)	Datenschutzbeauftragte in Stellen, die personenbezogene Daten verarbeiten, sind optional und reduzieren Meldepflicht (§18 (2))[29]	Datenschutzbeauftragte in Stellen, die personenbezogene Daten automatisiert verarbeiten, sind obligatorisch außer bei nicht-öffentlichen Stellen, die in der regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Die Bestellung winwa Datenschutzbeauftragten reduziert die Meldepflicht (§4d (2)), außer bei geschäftsmäßiger automatisierter Verarbeitung zum Zweck der Übermittlung (§4d (4))
Gefährdungshaftung für öffentlichen Bereich (§7) Verschuldenshaftung mit umgekehrter Beweislast für nichtöffentlichen Bereich (§8)	Gefährdungshaftung, Verschuldenshaftung mit umgekehrter Beweislast kann vorgesehen werden (§23)	Gefährdungshaftung für öffentlichen Bereich bei automatisierter Datenverarbeitung (§8) Sonst Verschuldenshaftung, sofern gebotene Sorgfalt nicht beachtet (§7)

[29] ausführlicher Kommentar hierzu: Martina Weber: Der betriebliche Datenschutzbeauftragte im Lichte der EG-Datenschutzrichtlinie; Datenschutz und Datensicherung DuD 19/12 (1995) 698-702.

European Commission Adopts Directive on Protection of Personal Data

---

EUROPEAN COMMISSION PRESS RELEASE: IP/95/822
DOCUMENT DATE: JULY 25, 1995

COUNCIL DEFINITIVELY ADOPTS DIRECTIVE ON PROTECTION OF PERSONAL DATA

The Directive on the protection of personal data has been formally adopted by the Council of Ministers. ``I am pleased that this important measure, which will ensure a high level of protection for the privacy of individuals in all Member States, has been adopted with a very wide measure of agreement within the Council and European Parliament'' commented Single Market Commissioner Mario Monti. ``The Directive will also help to ensure the free flow of Information Society services in the Single Market by fostering consumer confidence and minimising differences between Member States' rules. Moreover, the text agreed includes special provisions for journalists, which reconcile the right to privacy with freedom of expression,'' he added. ``The Member States must transpose the Directive within three years, but I sincerely hope that they will take the necessary measures without waiting for the deadline to expire so as to encourage the investment required for the Information Society to become a reality.''

The Directive will establish a clear and stable regulatory framework necessary to guarantee free movement of personal data, while leaving individual EU countries room for manoeuvre in the way the Directive is implemented. Free movement of data is particularly important for all services with a large customer base and depending on processing personal data, such as distance selling and financial services. In practice, banks and insurance companies process large quantities of personal data inter alia on such highly sensitive issues as credit ratings and credit-worthiness. If each Member State had its own set of rules on data protection, for example on how data subjects could verify the information held on them, cross-border provision of services, notably over the information superhighways, would be virtually impossible and this extremely valuable new market opportunity would be lost.

The Directive aims to narrow divergences between national data protection laws to the extent necessary to remove obstacles to the free movement of personal data within the EU. As a result, any person whose data are processed in the Community will be afforded an equivalent level of protection of his rights, in particular his right to privacy, irrespective of the Member State where the processing is carried out.

Until now, differences between national data protection laws have resulted in obstacles to transfers of personal data between Member States, even when these States have ratified the 1981 Council of Europe Convention on personal data protection. This has been a particular problem, for example, for multinational companies wishing to transfer data concerning their employees between their operations in different Member States.

Such obstacles to data transfers could seriously impede the future growth of Information Society services. As the Bangemann Group report to the Corfu European Council remarked: ``Without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine the rapid development of the information society.'' As a result, the Corfu European Council called for the rapid adoption of the data protection Directive.

To prevent abuses of personal data and ensure that data subjects are informed of the existence of processing operations, the Directive lays down common rules, to be observed by those who collect, hold or transmit personal data as part of their economic or administrative activities or in the course

of the activities of their association. In particular, there is an obligation to collect data only for specified, explicit and legitimate purposes, and to be held only if it is relevant, accurate and up-to-date.

The Directive also establishes the principle of fairness, so that collection of data should be as transparent as possible, giving individuals the option of whether they provide the information or not. Moreover, individuals will be entitled to be informed at least about the identity of the organisation intending to process data about them and the main purposes of such processing. That said, the Directive applies different rules according to whether information can be easily provided in the normal course of business activities or whether the data has been collected by third parties. In the latter case, there is an exemption where the obligation to provide information is impossible or involves disproportionate effort.

The Directive requires all data processing to have a proper legal basis. The six legal grounds defined in the Directive are consent, contract, legal obligation, vital interest of the data subject or the balance between the legitimate interests of the people controlling the data and the people on whom data is held (i.e. data subjects). This balance gives Member States room for manoeuvre in their implementation and application of the Directive.

Under the Directive, data subjects are granted a number of important rights including the right of access to that data, the right to know where the data originated (if such information is available), the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use their data in certain circumstances (for example, individuals will have the right to opt-out free of charge from being sent direct marketing material, without providing any specific reason).

In the case of sensitive data, such as an individual's ethnic or racial origin, political or religious beliefs, trade union membership or data concerning health or sexual life, the Directive establishes that it can only be processed with the explicit consent of the individual, except in specific cases such as where there is an important public interest (e.g. for medical or scientific research), where alternative safeguards have to be established.

As the flexibility of the Directive means that some differences between national data protection regimes may persist, the Directive lays down the principle that the law of the Member State where a data processor is established applies in cases where data is transferred between Member States.

The Directive also establishes arrangements for monitoring by independent data supervisory authorities, where necessary acting in tandem with each other.

In the specific case of personal data used exclusively for journalistic, artistic or literary purposes, the Directive requires Member States to ensure appropriate exemptions and derogations exist which strike a balance between guaranteeing freedom of expression while protecting the individual's right to privacy.

For cases where data is transferred to non-EU countries, the Directive includes provisions to prevent the EU rules from being circumvented. The basic rule is that the non-EU country receiving the data should ensure an adequate level of protection, although a practical system of exemptions and special conditions also applies. The advantage for non-EU countries who can provide adequate protection is that the free flow of data from all 15 EU states will henceforth be assured, whereas up to now each state has decided on such questions separately.

For their part, the Council and the Commission have made it clear that they consider that the European Union institutions and bodies should be subject to the same protection principles as those laid down in the Directive.

Anpassung des BDSG an die Datenschutzrichtlinie der EU

Mehr als zwei Jahre nach Ende der Frist, innerhalb derer die Bundesrepublik Deutschland die Datenschutzrichtlinie der EU in nationales Recht hätte umsetzen müssen und Ankündigung einer Klage der EU gegen die Bundesrepublik, war der zeitliche Druck ziemlich groß geworden. Deshalb wurde von der Regierungskoalition eine 2-stufige Modernisierung des BDSG geplant:

In einer 1. Stufe wurde das BDSG kurzfristig an die Datenschutzrichtlinie der EU angepasst, vgl. BDSG vom 23.05.2001, s.o..

In einer 2. Stufe sollte, möglichst noch in der damaligen Legislaturperiode, das BDSG grundlegend überdacht, überarbeitet und modernisiert werden. Die Bundestagsabgeordneten Cem Özdemir und Jörg Tauss beabsichtigten, diese Novellierungsdiskussion weitgehend via Internet zu dokumentieren, ja sogar zu führen. Das Bundesinnenministerium hat als Vorbereitung und wissenschaftliche Grundlage hierfür im Sommer 2000 bei Prof. Alexander Roßnagel, Prof. Hansjürgen Garstka und mir ein Gutachten „Modernisierung des Datenschutzrechts“ in Auftrag gegeben, das im September 2001 fertiggestellt wurde und unter `http://www.bmi.bund.de` →`Publikationen` →nach „`Datenschutz`“ suchen verfügbar ist (direkter Link: `http://www.bmi.bund.de/cln_028/nn_121894/Internet/Content/Common/Anlagen/Broschueren/2001/Modernisierung__des__Datenschutzrechts__Id__11659__de,templateId=raw,property=publicationFile.pdf/Modernisierung_des_Datenschutzrechts_Id_11659_de`).

Organisation for Economic Co-Operation and Development (OECD)

OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

O.E.C.D. Document C(80)58(Final), October 1, 1980

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

Adopted by the Council 23rd September, 1980

The Council,
Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

Recognising:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

ANNEX

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
   b) "personal data" means any information relating to an identified or identifiable individual (data subject);
   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:
   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

a) as few as possible, and

b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject:

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
    i) within a reasonable time;
    ii) at a charge, if any, that is not excessive;
    iii) in a reasonable manner; and
    iv) in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;
b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
c) provide for reasonable means for individuals to exercise their rights;
d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

i) information exchange related to these Guidelines, and

ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

APPENDIX

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

EXPLANATORY MEMORANDUM

Introduction

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.

The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions. The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

I GENERAL BACKGROUND

The Problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

Activities at national level

... (hier geht’s noch ca. 20 Druckseiten weiter)

Organisation for Economic Co-Operation and Development: Guidelines for the Security of Information Systems; OECD / GD (92)190, Paris 1992.

1990 wurde eine Expertengruppe unter dem Vorsitz von Hon. Michael Kirby eingerichtet; Der Entwurf der Richtlinie wurde von Ms. Deborah Hurley nach den Anregungen dieser Expertengruppe geschrieben.

OECD ADOPTS GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

The 24 OECD Member countries on 26th November 1992 adopted Guidelines for the Security of Information Systems, culminating almost two years' work by an OECD expert group composed of governmental delegates, scholars in the fields of law, mathematics and computer science, and representatives of the private sector, including computer and communication goods and services providers and users.

The term information systems includes computers, communication facilities, computer and communication networks and the information that they process. These systems play an increasingly significant and pervasive role in a multitude of activities, including national economies, international trade, government and business operation, health care, energy, transport, communications and education.

Security of information systems means the protection of the availability, integrity, and confidentiality of information systems. It is an international issue because information systems frequently cross national boundaries.

While growing use of information systems has generated many benefits, it has also shown up a widening gap between the need to protect systems and the degree of protection currently in place. Society has become very dependent on technologies that are not yet sufficiently dependable. All individuals and organizations have a need for proper information system operations (e.g. in hospitals, air traffic control and nuclear power plants).

Users must have confidence that information systems will be available and operate as expected without unanticipated failures or problems. Otherwise, the systems and their underlying technologies may not be used to their full potential and further growth and innovation may be prohibited.

The Guidelines for the Security of Information Systems will provide the required foundation on which to construct a framework for security of information systems. They are addressed to the public and private sectors and apply to all information systems. The framework will include policies, laws, codes of conduct, technical measures, management and user practices, ad public education and awareness activities at both national and international levels.

Several OECD Member countries have been forerunners in the field of security of information systems. Certain laws and organizational and technical rules are already in place. Most other countries are much farther behind in their efforts. The Guidelines will play a normative role and assist governments and the private sector in meeting the challenges of these worldwide systems. The Guidelines bring guidance and a real value-added to work in this area, from a national and international perspective.

The OECD Security Guidelines are similar in form to the 1980 OECD Privacy Guidelines and will probably have a substantial impact on security policy.

Of course, there are lots of issues left open by the Guidelines, including the relationship between privacy and security. But the principles offer a good starting point for public discussion on security and risks-related issues.

Recommendation of the Council Concerning Guidelines for the Security of Information Systems, 26 November 1992

...

Recommends that member countries

1. establish measures, practices and procedures to reflect the principles concerning the security of information systems set forth in the Guidelines contained in the Annex to this Recommendation, which is an integral part hereof;
2. consult, co-ordinate and co-operate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices and procedures for the security of information systems;
3. agree as expeditiously as possible on specific initiatives for the application of the Guidelines;
4. disseminate extensively the principles contained in the Guidelines;
5. review the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems.

Guidelines for the Security of Information Systems

I. AIMS

...

II. SCOPE

... addressed to the public and private sectors.
... apply to all information systems.
... capable of being supplemented by additional practices and procedures

III. DEFINITIONS

...
confidentiality ... disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner;
...

IV. SECURITY OBJECTIVE

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

V. PRINCIPLES

1. Accountability Principle

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principle

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures practices and procedures for the security of information systems should take into account of and address all relevant consideration and viewpoints, including technical, administrative, organizational, operational, commercial, educational and legal.

5. Proportionality Principle
Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle
Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organization so as to create a coherent system of security.

7. Timeliness Principle
Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of information systems.

8. Reassessment Principle
The security information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle
The security of information systems should be compatible with the legitimate use and flow of data ad information in a democratic society.

VI. IMPLEMENTATION
... (2 Seiten)

EXPLANATORY MEMORANDUM to Accompany the Guidelines for the Security of Information Systems
... (ca. 22 Seiten)

Vereinte Nationen: Richtlinien betreffend personenbezogene Daten in automatisierten Dateien

von der Generalversammlung beschlossen am 4. Dezember 1990[30]

Die Verfahrensweisen für die Anwendung der Bestimmungen bezüglich personenbezogener Daten in automatisierten Dateien werden der Initiative der einzelnen Staaten überlassen. Sie müssen sich jedoch an folgenden Grundsätzen orientieren:

A. Grundsätze betreffend den Mindeststandard, der durch die nationale Gesetzgebung gewährleistet werden sollte

1. Grundsatz der Rechtmäßigkeit und der Beachtung von Treu und Glauben

[30] zitiert nach: Ulrich Dammann, Spiros Simitis: Bundesdatenschutzgesetz (BDSG) mit Landesdatenschutzgesetzen und Internationalen Vorschriften; 5. Auflage, Nomos Verlagsgesellschaft, Baden-Baden 1991

Personenbezogene Informationen sollten nicht auf rechtswidrige Weise oder unter Verstoß gegen Treu und Glauben erhoben oder verarbeitet werden, noch sollten die Informationen für Zwecke verwendet werden, die im Gegensatz zu den Zielsetzungen und Grundsätzen der Charta der Vereinten Nationen stehen.

2. Grundsatz der Richtigkeit

Die für die Zusammenstellung und Führung von Dateien verantwortlichen Personen sind dazu verpflichtet, die Richtigkeit und Relevanz der erfaßten Daten regelmäßig zu überprüfen und dafür Sorge zu tragen, dass sie, um Irrtümer und Auslassungen zu vermeiden, so vollständig wie möglich geführt und regelmäßig oder anläßlich der Verwendung der in der Datei gespeicherten Angaben auf den neuesten Stand gebracht werden, solange mit den Daten gearbeitet wird.

3. Grundsatz der Zweckbestimmung

Der Zweck, dem eine Datei dienen soll, und deren dementsprechende Verwendung sollten genau bestimmt werden, rechtmäßig sein, und eine Datei sollte bei ihrer Einrichtung zu einem gewissen Grad öffentlich bekannt gemacht oder der Betroffene davon in Kenntnis gesetzt werden. Dadurch soll anschließend sichergestellt werden können, dass

a) alle erhobenen und erfaßten personenbezogenen Daten für die solcherart festgelegten Zwecke relevant und angemessen bleiben;
b) keine der genannten personenbezogenen Daten für Zwecke, die im Widerspruch mit den solcherart festgelegten Zwecken stehen, genutzt oder übermittelt werden, es sei denn, der Betroffene hat eingewilligt;
c) der Zeitraum, über den die personenbezogenen Daten gespeichert bleiben, nicht länger ist als der Zeitraum, der zur Erfüllung des solcherart festgelegten Zwecks erforderlich ist.

4. Grundsatz der Möglichkeit des Betroffenen zur Einsichtnahme

Jeder, der seine Identität nachweist, hat das Recht, Kenntnis davon zu erlangen, ob seine Person betreffende Informationen verarbeitet werden und sie ohne unangemessene Verzögerung oder Kosten in verständlicher Form zur Verfügung gestellt zu bekommen sowie im Falle unrechtmäßiger, nicht erforderlicher oder ungenauer Eintragungen eine entsprechende Berichtigung bzw. Löschung zu erwirken und über die Adressaten in Kenntnis gesetzt zu werden, falls die Informationen weitergegeben werden. Entsprechende Rechtsmittel sollten festgelegt werden, und, falls erforderlich, sollte die in Grundsatz 8 aufgeführte Aufsichtsbehörde angegeben werden. Die Kosten einer Berichtigung sind von den für die Datei verantwortlichen Personen zu tragen. Es wäre wünschenswert, dass die Bestimmungen ungeachtet der Staatsangehörigkeit und des Wohnsitzes für alle Personen gelten.

5. Grundsatz der Nichtdiskriminierung

Vorbehaltlich der restriktiv im Grundsatz 6 niedergelegten Ausnahmen sollten Daten, die leicht zu ungesetzlicher oder willkürlicher Diskriminierung führen können, u.a. Angaben über rassische oder ethnische Herkunft, Hautfarbe, Sexualleben, politische Anschauungen, religiöse, weltanschauliche und andere Überzeugungen sowie die Mitgliedschaft in einer Vereinigung oder einer Gewerkschaft, nicht erfaßt werden.

6. Ausnahmebefugnisse

Abweichungen von der Anwendung der unter 1-4 genannten Grundsätze dürfen nur zugelassen werden, wenn sie erforderlich sind, um die nationale Sicherheit, die öffentliche Ordnung, die öffentliche Gesundheit oder Moral wie auch die Rechte und Freiheiten anderer, insbesondere verfolgter Personen (humanitärer Vorbehalt), zu schützen, falls diese Abweichungen ausdrücklich durch Gesetz oder entsprechende Regelungen festgelegt sind. Diese Gesetze oder Regelungen müssen in Übereinstimmung mit der Rechtsordnung des jeweiligen Staates ausdrücklich die Grenzen dieser Ausnahmen festlegen und einen angemessenen Schutz gewährleisten.

Abgesehen davon, dass für sie die für Ausnahmen von den Grundsätzen 1 bis 4 vorzusehenden Schutzbestimmungen bestehen müssen, dürfen Ausnahmen von dem im Grundsatz verankerten Verbot der Diskriminierung nur zugelassen werden, wenn sie mit der Allgemeinen Erklärung der Menschenrechte und der Verhütung von Diskriminierung vereinbar sind.

7. Grundsatz der Sicherheit

Geeignete Maßnahmen sollten ergriffen werden, um die Dateien sowohl gegen Naturgefahren, wie zufälligen Verlust oder Zerstörung, als auch gegen Gefahren durch menschliche Einwirkungen, wie z.B. unerlaubten Zugang, vorsätzlichen Mißbrauch von Daten oder das Einsetzen von Computerviren, zu schützen.

8. Überwachung und Sanktionen

Im Gesetz des jeweiligen Landes ist festzulegen, welche Stelle in Übereinstimmung mit der Rechtsordnung des jeweiligen Staates dafür zuständig sein soll, die Einhaltung der obigen Grundsätze zu überwachen. Diese Stelle muss Garantien für Unparteilichkeit, für Unabhängigkeit gegenüber den für die Verarbeitung und Erhebung verantwortlichen Personen oder Behörden und fachliche Kompetenz bieten. Für den Fall der Verletzung der nationalen Rechtsvorschriften, die zur Verwirklichung der vorgenannten Prinzipien geschaffen worden sind, sollten strafrechtliche Maßnahmen oder andere Sanktionen und die jeweils angemessenen Rechtsmittel vorgesehen werden.

9. Grenzüberschreitender Datenverkehr

Sofern bei einem grenzüberschreitenden Datenverkehr die Gesetzgebungen zweier oder mehrerer betroffener Staaten vergleichbare Sicherungen für den Schutz der Privatsphäre bieten, sollten die Informationen zwischen ihnen so frei wie innerhalb jedes Einzelstaates ausgetauscht werden können. Wenn keine entsprechenden Schutzbestimmungen bestehen, dürfen Beschränkungen für diesen Austausch nicht unangemessenerweise und nur insoweit verfügt werden, als der Schutz der Privatsphäre es erfordert.

10. Geltungsbereich

Die obigen Bestimmungen sollten in erster Linie für alle öffentlichen und privaten automatisierten Dateien einschließlich manueller Dateien gelten, für die diese Bestimmungen auf der Basis einer freiwilligen Ausweitung und unter dem Vorbehalt entsprechender Anpassungen Gültigkeit haben sollten. Ebenfalls auf freiwilliger Basis könnten spezielle Bestimmungen geschaffen werden, wodurch alle oder ein Teil der Grundsätze auch für Dateien über juristische Personen gelten sollen, besonders dann, wenn diese Angaben über Einzelpersonen enthalten.

B. Anwendung der Richtlinien auf personenbezogene Daten in den Dateien internationaler staatlicher Organisationen

Die vorliegenden Richtlinien sollten für personenbezogene Daten in Dateien staatlicher internationaler Organisationen gelten, vorbehaltlich etwa erforderlicher Anpassungen in bezug auf eventuelle Unterschiede, die zwischen Dateien für interne Zwecke, wie z.B. die Personalverwaltung betreffende Dateien, und Dateien für externe Zwecke bestehen könnten, die sich auf Dritte beziehen, welche mit der Organisation in Verbindung stehen.

Jede Organisation sollte eine Behörde benennen, die eine gesetzliche Zuständigkeit für die Überwachung der Einhaltung dieser Regelungen besitzt.

Humanitärer Vorbehalt: Eine Abweichung von diesen Prinzipien kann für Dateien vorgesehen werden, deren Zweck auf den Schutz der Menschenrechte und Grundfreiheiten des einzelnen oder humanitäre Hilfe gerichtet ist.

Eine entsprechende abweichende Bestimmung sollte in der nationalen Gesetzgebung für die staatlichen internationalen Organisationen vorgesehen werden, deren Abkommen über den Sitz der Organisation nicht die Anwendung der genannten nationalen Gesetzgebung ausschließt, sowie für die nichtstaatlichen internationalen Organisationen, für welche dieses Gesetz Anwendung findet.

Weitere Materialien

Weiter Materialien, insbesondere zu Datenschutzregelungen anderer Länder, finden Sie unter:
`http://www.datenschutz-berlin.de/`

Grundsätzliches Defizit der bisherigen Datenschutzregelungen aus meiner Sicht

Alle bisherigen Datenschutzregelungen knüpfen an **personenbezogenen *Daten*** an und bewegen sich damit unausgesprochen in der von Claude Shannon geschaffenen ***informationstheoretischen Modellwelt***, vgl. die Vorlesung „Informations- und Kodierungstheorie“ und mein Skript zu „Datensicherheit“.

Für die Praxis können jedoch ***Aufwandsaspekte*** nicht vernachlässigt werden – sie sind oftmals entscheidend. Wichtig ist also auch, welche Funktionen auf den personenbezogenen Daten mit welchem Aufwand, d.h. innerhalb welcher Zeit und unter Inkaufnahme welcher Kosten, ausgeführt werden können.

Ein Beispiel hierfür ist die zur Zeit heftig diskutierte **Telefonnummern-CD-ROM**. Selbst wenn sie im informationstheoretischen Sinne nichts anderes als die gedruckten öffentlichen Telefonbücher enthält (und ihre Herstellung, ihr Vertrieb und ihre Nutzung damit wahrscheinlich nicht gegen Datenschutzregelungen verstößt, da alle Daten auf ihr öffentlich sind[31]) bringt die Möglichkeit, mit geringem Aufwand nicht nur

---

[31] vgl. BDSG §28 (1) 3. sowie §29 (1) 2.; Datenschutzrichtlinie der EU vom 24.07.1995, §8 2 e);
im BDSG §43 wird Strafe allerdings daran geknüpft, ob die personenbezogenen Daten „offenkundig“ sind. Dies ist aus Sicht mancher etwas anderes als „öffentlich“ zugänglich:

> Das baden-württembergische Innenministerium hat die Beschwerdeführer auf die Strafbarkeit der Veröffentlichung von D-Info hingewiesen.
>
> Nach BDSG Par. 43 Abs. 1 ist das illegale Speichern, Verändern und Übermitteln von personenbezogenen Daten strafbar, die nicht offenkundig sind.
>
> Das Innenministerium hält den zusätzlichen Informationsinhalt (Suche nach Telefonnummer, Auflisten von Strassen..) für nicht offenkundig.
>
> Strafantrag kann formlos bei der zuständigen Staatsanwaltschaft Mannheim (Postfach 68149 Mannheim) gestellt werden. Das kann jede(r) tun, der/die im Telefonbuch steht. Frist beachten: 3 Monate nach dem ihr von der Strafbarkeit Kenntnis erlangt.

- zu einem Namen mit Wohnort die Telefonnummer,

sondern auch

- zu einer Telefonnummer den Namen mit Wohnort

zu ermitteln, eine drastische Änderung.

So etwas ist prinzipiell nur in einer ***komplexitätstheoretischen Modellwelt*** (mit ziemlich genauer Modellierung des Aufwands) beschreibbar – und damit grundsätzlich außerhalb dessen, was an der informationstheoretischen Sicht orientierter Datenschutz regeln kann.

Nun gibt es in den bisherigen Datenschutzregelungen durchaus Aspekte, die in diese komplexitätstheoretische Richtung gehen: Einerseits die *Zweckbindung*, d.h. Daten *dürfen* nur für die Zwecke verwendet werden, für die sie erhoben wurden[32]. Andererseits die Unterscheidung zwischen Akten und Dateien bzw. nicht automatisierten und automatisierten Dateien[33]. Erstere sind in der Benutzung umständlicher, so dass sie – etwa bzgl. Auskunftsrechten – weniger scharf reglementiert werden. Wünschenswert wäre nun, dass Zweckbindung nicht nur das *Dürfen*, sondern auch das *Können* regelt und beim Umgang mit öffentlichen personenbezogenen Daten nicht rein informationstheoretisch gedacht wird, sondern auch hier funktionsbezogen: Erweiterungen der faktischen Möglichkeiten oder Effizienzverbesserungen im Umgang mit öffentlichen personenbezogenen Daten sollten, zumindest soweit es um staatliche oder kommerzielle Tätigkeiten geht, vom Datenschutz geregelt werden.

Quelle: Datenschutz Nachrichten 1-1996 Hrg.: Deutsche Gesellschaft f. Datenschutz, Reuterstraße 44, 53113 Bonn, Fax: 0228/241352

[32] vgl. BDSG §4 (2) sowie §14, §15 (3), §16 (4), §17 (4), §28 (4), §39; OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) Purpose Specification Principle (9.) und Use Limitation Principle (10.); Vereinte Nationen: Richtlinien betreffend personenbezogene Daten in automatisierten Dateien (4. Dezember 1990) A. 3. Grundsatz der Zweckbestimmung

[33] BDSG §1 (3) 2. sowie §3 (2)

Verantwortung

Das folgende Material geht vom Allgemeinen zum Speziellen:

Zunächst werden zwei Lexikonauszüge „Verantwortung“ wiedergegeben, ein kurzer und ein sehr ausführlicher. Als ergänzende Lektüre empfehle ich: Rupert Leitner: Responsibility and Uncertainty, http://www.europaeische-akademie-aw.de/pages/publikationen/newsletter/50.pdf

Danach ein kurzer Artikel über die Sicht EDWARD TELLERs, des „Vaters der Wasserstoffbombe“, zur Verantwortung des Wissenschaftlers. Diese Sicht ist meiner Meinung nach extrem – mit starker Tendenz zu extremistisch bis gemeingefährlich.

Schließlich fasse ich die wesentlichen Thesen von DAVID LORGE PARNAS zur Beruflichen Verantwortung von Software-Ingenieuren zusammen. Sie bilden den Gegenpol zur Sicht von EDWARD TELLER und stammen aus

Parn1_94 D. L. Parnas: Professional Responsibilities of Software Engineers; Klaus Brunnstein, Eckart Raubold: Technology and Foundations; IFIP 13th World Computer Congress 94, Volume 2, Elsevier Science B.V., Amsterdam 1994, 332-339.

Zwei Lexikonauszüge „Verantwortung“

Verantwortung, urspr. v.a. in der Rechtsprechung verwendeter Terminus zur Bez. des Rechenschaftgebens für ein bestimmtes Handeln oder für dessen Folgen. Als soziale Beziehungsstruktur umfaßt V. einen Träger, einen Bezugspunkt (V. für Person[en] oder Sache[n]) und eine Legitimationsinstanz (V. vor Person[en] oder Transzendentem). V. setzt Mündigkeit voraus, d.h. die Fähigkeit, das eigene Handeln frei zu bestimmen und dessen Folgen abzusehen.

aus: *Meyers Grosses Taschenlexikon in 24 Bänden, BI, 4. vollst. überarb. Auflage, 1992*

Verantwortung, ein im 20. Jh. in das Zentrum eth. und ethisch-polit. Diskurse, aber auch der polit. und publizist. Rhetorik getretener Begriff zur Bez. einer selbst eingegangenen und von anderen zugewiesenen moral. Verpflichtung zur gewissenhaften Pflichten- und Folgenabwägung in konflikthaften Entscheidungen. ›Verantworten‹ stammt urspr. aus der spätmittelalterl. Gerichtssprache und bedeutet, gegenüber einem Richter für sein Tun Rechenschaft abzulegen, es zu begründen und zu verteidigen. Die Kategorie V. als ein Schlüsselbegriff der heutigen Zeit ist im Kontext der Ethik entstanden und taucht hier erst seit den 1930er Jahren auf.

Verantwortung als ethisches Problem

Dem Wortsinn nach bezeichnet V. eine dreistellige Relation: *Jemand* ist für *etwas* gegenüber *einer Instanz* verantwortlich. ›V. tragen‹ heißt also: bereit sein oder genötigt werden, sich zu ›verantworten‹, jemandem für etwas, in bezug auf etwas zu antworten. Dementsprechend wirft die ethische V.-Problematik folgende Grundfragen auf:

1) *Wer* ist unter welchen Bedingungen verantwortungsfähig und verantwortungspflichtig?
2) *Wem* ist einer verantwortlich, *welche Instanz* kann Rechenschaft fordern?
3) Worauf bezieht sich die V., was ist *Gegenstand* von Verantwortung?

1) Als im philosoph. und christlich-theolog. Sinne verantwortungsfähig gilt allein der individuelle Mensch als zur freien Entscheidung befähigte Person. Es gibt weder eine Kollektivschuld noch eine moral. Kollektiv-V.; moral. V. kann nicht übertragen oder zw. Individuen aufgeteilt werden. Im Sinne einer Mit-V. kann V. jedoch gemeinsam getragen werden. Als verantwortlich gilt der Mensch nur insoweit, als er in seinem Tun frei ist, ihm also mehrere Möglichkeiten des Handelns von unterschiedl. moral. Qualität offenstehen.

2) V.-Diskurse unterscheiden sich v.a. hinsichtlich der Instanz, der gegenüber der Mensch verantwortlich erscheint. In der Jurisprudenz ist dies der Richter als Repräsentant der Rechtsgemeinschaft, in der Theologie Gott als liebender Schöpfer des Menschen und der Welt. Im Horizont des modernen Autonomiedenkens bestimmt die philosoph. Ethik den Menschen als in erster Linie vor sich selbst verantwortlich. V. erscheint hier als Korrelat menschl. Freiheit und als Ergebnis einer Selbstverpflichtung des Menschen, als deren Instanz das Gewissen gilt.
3) Was als Gegenstand von Verantwortung gelten kann, ist kontext- und situationsabhängig, beruht jedoch stets auf normativen Urteilen über Gut und Böse bzw. über Güter und Übel. Normative Urteile sind aber nur eine notwendige, keine hinreichende Bedingung für das Entstehen von V. Hinzutreten muss ein Zurechnungsurteil, das ein bestimmtes normativ bewertetes Ereignis (eine Handlung, einen Schaden, einen Erfolg) einer bestimmten Person kausal und i.d.R. auch intentional zurechnet.

Unter V.-Ethik wird seit M. WEBER ein eth. Diskurs verstanden, der den moral. Wert von Entscheidungen oder Handlungen an der Qualität der Güterabwägung und der angemessenen Beachtung der mögl. Folgen mißt. Im Unterschied dazu finden in der Gesinnungsethik primär die Intention des Handelnden und deren Übereinstimmung mit allg. verbindl. Pflichten Beachtung. Wenn aber nur der moral. Wert der Einzelhandlung und das eigene Gewissen als Instanz der V.-Kontrolle anerkannt werden, verliert V. den Charakter des Rechenschaftgebens, das als ›Antwort‹ stets nur Dritten gegenüber möglich ist. Der philosoph. V.-Diskurs hat zu begründen, warum der Mensch eine moral. Pflicht zur Selbstverpflichtung und zur Rechenschaft auch gegenüber Dritten hat. Hierzu liegen subjekt- (W. SCHULZ) und geschichtsphilosoph. (G. PICHT), werteth. (H. JONAS), theolog. (F. BÖCKLE), prinzipienorientierte (H. LENK), diskurstheoret. (K. O. APEL) und tauschtheoret. (OTFRIED HÖFFE) Argumentationen vor.

Aus jurist. und soziolog. Sicht ist V. primär das Produkt von Zuschreibungen Dritter. Mit der anerkennenden Zuweisung oder krit. Einforderung von V. wird an die moral. Bereitschaft zur Selbstverpflichtung appelliert. Ohne Selbstverpflichtung könnte es in komplexen und hochindividualisierten Gesellschaften keine verlässl. Sozialbeziehungen geben.

Die meisten prakt. Phänomene von V. sind sowohl Ergebnis von Selbstverpflichtung als auch von Fremdzuschreibungen. Dies ist offensichtlich bei allen Arten von Verträgen und organisationsinternen Aufträgen (Aufgaben-V.) oder bei der Übernahme von Wahlämtern (polit. V.). Auch generelle oder nichtvertragliche spezif. Rechtspflichten (z.B. im Familienrecht) werden i.d.R. im Sinne einer Selbstverpflichtung übernommen.

Zeitgeschichtliche Bedeutung

Die traditionelle Ethik ging von einem einfachen Modell menschl. Handelns aus, dessen Reichweite bei den unmittelbaren, für jedermann einsichtigen Ergebnissen endete. Die Handlungsbedingungen moderner Gesellschaften zeichnen sich jedoch durch eine Verlängerung und Vernetzung von Handlungsketten aus, d.h., die Handlung eines einzelnen steht in einem größeren, arbeitsteiligen und oft folgenreichen Zusammenhang und gewinnt darin erst ihren Sinn. Die Stabilisierung solcher komplexen Zusammenhänge in der Neuzeit wurde möglich durch

1) die Ausdifferenzierung und institutionelle Verselbständigung der großen Sinnsphären von Wirtschaft, Politik, Religion, Wiss. und Familie; sie lassen sich als gesellschaftl. Teilsysteme mit spezif., für sie charakterist. Wertorientierungen, Interaktionsstilen und Organisationsformen verstehen;
2) die Entstehung der modernen, auf temporärer und nicht exklusiver Mitgliedschaft von Personen beruhenden Organisation.

So werden bestimmte Handlungen eindeutig einer Sinnsphäre zugeordnet und damit von anderen Rücksichten (z.B. polit., familialer oder religiöser Art) entlastet. Wenn Personen Mitgl. in

wirtschaftl., polit. u.a. Organisationen werden, erhalten sie bestimmte Positionen oder Aufgaben, durch die ihre Rechte und Pflichten und damit auch ihre V. bestimmt und begrenzt werden. Für den einzelnen bedeutet dies, dass er in unterschiedl. V.-Zusammenhänge zugleich hineingestellt ist (z.B. als Vater, Angestellter, Politiker), wobei auch Gewissens- oder V.-Konflikte bei versch., miteinander kollidierenden Pflichten entstehen können. Die Funktions- und Arbeitsteilung hat sich als außerordentlich erfolgreich erwiesen, aber sie wird mit einer Komplexitätssteigerung der Zusammenhänge erkauft, deren Problematik heute zunehmend bewußt wird.

Während im Horizont von Aufklärung und Liberalismus der Anspruch auf Eigen-V. als Ausdruck personaler Autonomie gegen das herrschende paternalist. Denken in Kirche und Staat öffentlich artikuliert wurde, wird in den öffentl. Diskursen heute vielfach die V. ›der anderen‹ gefordert (z.B. im Zusammenhang mit ökolog. und technolog. Risiken). Bedingungen hierfür sind die zunehmende Reichweite unseres Kausalwissens sowie die Vielfalt damit verbundener Zurechnungsmöglichkeiten einerseits und die zunehmende Wahrnehmung problem. Nebenfolgen techn. und ökonom. Fortschritte andererseits. Die Verselbständigung der Sinnsphären und der Organisationen führt dazu, dass bei Entscheidungen ihre systemexternen Effekte nur insoweit wahrgenommen werden, als sie nachträglich auf das System, in dem die Entscheidungen fallen, zurückwirken. Die Ausblendung der Nebenwirkungen auf andere Bereiche (z.B. des Wirtschaftswachstums auf die natürl. Umwelt oder des Fernsehens auf die kindl. Entwicklung) bildet den strukturellen Grund für den vermehrten Ruf nach V. im Sinne einer umfassenderen Folgenorientierung von Entscheidungen. Aber weil bestimmte Wirkungen häufig nicht eindeutig auf bestimmte Handlungen oder Entscheidungen rückführbar sind und zudem die Instanzen fehlen, die (wie z.B. Menschenrechtsorganisationen in bezug auf die Wahrung der Menschenrechte) Rechenschaft fordern können, lassen sich die drohenden Gefahren und auszutragenden Folgen der Modernisierung häufig schwer als V.-Probleme behandeln. Niemand kann eine unabgegrenzte V. übernehmen.

Verantwortung und Verantwortlichkeit

Arbeitsteilung (z.B. in der Geschäftsleitung eines Unternehmens oder in der Regierung) führt zu einer Diffusion der V. Jeder Beteiligte kann nur einen Ausschnitt der in Frage stehenden Gesamtabläufe überblicken und ist für die Abwägung versch. Aspekte auf die Einschätzung Dritter angewiesen. So gehen wiss. Entdeckungen, z.T. vermittelt durch polit. Entscheidungen, in techn. Nutzung über. Wissenschaftler, Politiker und Techniker(gruppen) sind dann z.B. an der Einführung eines Produktes beteiligt, das insbesondere bei schädl. Neben- oder Folgewirkungen vor der Öffentlichkeit zu verantworten ist. Aus der Sicht der von negativen Folgen Betroffenen kommt es dabei nicht auf die Absicht derjenigen an, die z.B. über das neue Produkt oder Gesetz entscheiden, sondern auf die für sie erfahrbaren Wirkungen. Diese sind aber nicht von den einzelnen beteiligten Individuen, sondern vom Handlungszusammenhang als ganzem abhängig. Da nur Personen und nicht organisierte Zusammenhänge im eth. Sinne verantwortlich sein können, bedarf das urspr. individualethisch orientierte Konzept der V. einer Erweiterung und Differenzierung, um heute praktisch wirksam zu sein.

Älter als in der Ethik ist das V.-Konzept im Recht. Insoweit rechtl. V.-Zuschreibung am Erfordernis von Schuld festhält, wie dies bes. für das Strafrecht charakteristisch ist, bleibt die Nähe zur eth. Auffassung gewahrt. Bereits die zivilrechtl. V. hebt nicht auf die Schuldhaftigkeit im Einzelfall, sondern auf die Vermeidbarkeit eines Schadens am Maßstab eines typ., allg. erwarteten Falls ab. Bei der → Gefährdungshaftung, wie sie z.B. für Betreiber von Kraftfahrzeugen oder für die Fabrikhaftpflicht charakteristisch ist, wird schließlich für die Folgen des gefährl. Betriebs an sich gehaftet, unabhängig von jedem Verschulden des Betreibers.

Im Sinne einer Differenzierung von V.-Ebenen lassen sich institutionelle oder Organisations-V., Führungs-V., Aufgaben-V. und individuelle Verantwortlichkeit unterscheiden. Da Organisationen

als kooperative Akteure nicht im moral., sondern nur im rechtl. Sinne schuldig werden können, bietet sich zur Operationalisierung der **Organisations-V.** das Prinzip der Gefährdungshaftung an, wie sie in Dtl. z.B. im Produkthaftungs-Ges. vom 15.12.1989 rechtlich verankert ist. Die **Führungs-V.** betrifft die Ausrichtung einer Organisation auf bestimmte Ziele, die Schaffung einer internen Aufgaben- oder V.-Struktur und die Beauftragung geeigneter Personen mit diesen Aufgaben. Die Führungs-V. ist nicht auf die Erfüllung bestimmter Pflichten gerichtet, sondern auf den ›richtigen‹ Gebrauch von Macht im Sinne erfolgreicher Entscheidungen. Nicht nur Machtmißbrauch, sondern auch mangelnder Erfolg ist dabei ein Rechenschaftsgrund. Die **Aufgaben-V.** steht im Schnittpunkt organisator. und persönl. V. Mit der Übernahme einer Aufgabe verpflichten sich Personen, den damit verbundenen normativen Erwartungen nach bestem Vermögen zu entsprechen. Allerdings werden nur solche Aufgaben als verantwortungsvoll bezeichnet, bei denen eine bloße Pflichterfüllung nicht ausreicht, sondern Handlungs- und Ermessensspielräume das eigenständige Entscheiden der Aufgabenträger erforderlich machen. Eine Aufgabe gilt als um so verantwortungsvoller, je größer der Zuständigkeitsbereich und je erheblicher die Folgen der zu treffenden Entscheidungen sind. Die Größe der V. ist somit von der Höhe des Entscheidungsrisikos abhängig. Mit der Zuweisung von Führungs- und Aufgaben-V. ist die Erwartung Dritter verbunden, dass die V.-Träger Entscheidungen treffen, an denen jene ein Interesse haben. Die Zuweisung von V. erteilt diese Macht und stellt zugleich einen Akt des Vertrauens dar, der an die Annahme bestimmter persönl. Fähigkeiten des V.-Trägers, seine Verantwortlichkeit, gebunden ist. Zwar besitzt diese einen moral. Kern, der sich in der Gewissenhaftigkeit der Pflichten- und Güterabwägung sowie der Zurückstellung eigener Interessen äußert; je komplexer die Entscheidungssituation, um so mehr gewinnt jedoch die erforderl. kognitive Kompetenz, d.h. die Fähigkeit, Vorgänge zu verstehen, sie zu planen, durchzuführen und zu beurteilen, an Bedeutung; schließlich bedarf es zur Anerkennung von Verantwortlichkeit auch einer angemessenen kommunikativen Begründung und Rechtfertigung getroffener Entscheidungen, bei denen es i.d.R. um Interessen- und Güterabwägungen geht, welche nicht alle, die davon betroffen sind, gleichermaßen befriedigen können.

Schuld, Haftungsverantwortung und Entscheidungsverantwortung

Die Ambivalenz des Rufs nach V. wird sichtbar, wenn man die Zeitstrukturen unterschiedl. V.-Begriffe betrachtet. Die rechtl. V. bezieht sich auf vergangene Ereignisse, entweder auf Handlungen, die Rechtsnormen verletzt haben (Schuld), oder auf entstandene Schäden, die einem Verursacher zugerechnet werden (Haftung). Die Pflicht, sich für pflichtverletzende oder Dritte schädigende Handlungen zur Rechenschaft ziehen zu lassen, ist grundsätzlich unstrittig; strittig ist lediglich in vielen Fällen die Zurechenbarkeit bestimmter Ereignisse auf bestimmte Handlungen oder einen bestimmten Täter. V. im Sinne des Eingehens von Entscheidungsrisiken, die von Entscheidungsträgern in Wirtschaft, Wissenschaft und Politik erwartet wird, ist dagegen zukunftsbezogen. Lediglich die vorhersehbaren möglichen Folgen können Gegenstand der Entscheidungs-V. sein, sie müssen bewertet und gegeneinander abgewogen werden; der Erfolg der Entscheidung wird sich erst später herausstellen.

Wer V. für eine Entscheidung übernimmt, geht von der Annahme eines Überwiegens der positiven Folgen aus. Wird nun versucht, durch eine Erweiterung der Rechtspflichten den Bereich der für eine Entscheidung möglicherweise negativen Handlungsfolgen zu vergrößern, so muss damit gerechnet werden, dass die Bereitschaft, Entscheidungs-V. zu übernehmen, sinkt. Die polit. Ausgestaltung des Haftungsrechts steht daher stets vor der Frage, inwieweit einem Akteur die mögl. negativen Folgen seiner Entscheidungen bzw. Handlungen zugerechnet werden sollen, und zwar unter dem Doppelaspekt der Gerechtigkeit und der Schadensverhütung einerseits und des Interesses am Zustandekommen bestimmter Entscheidungen andererseits.

Bedingungen verantwortlichen Handelns
Zur Unterstützung wichtiger Entscheidungen über Handlungsziele und Verfahrenswege etwa in Politik, Wirtschaft oder Forschung können Experten (z.B. → Politikberatung), Ethikkommissionen wie auch Kriterien der Folgenabschätzung in den Diskurs einbezogen werden. Interdisziplinarität des Diskurses ermöglicht zudem anthropolog., psycholog. und ökolog. Erwägungen darüber, welche Rückwirkungen technisch-lebensweltl. Veränderungen auf Mensch und Natur haben. Da aber auch das Einbeziehen von Expertenwissen und -meinungen (u.a. weil sogar die Aussagen von Experten derselben Fachrichtung oftmals differieren) keine Gewähr für die Richtigkeit einer Entscheidung bietet, können Lösungen nur im gewissenhaften, von Partikularinteressen möglichst befreiten Abwägen des Für und Wider gesucht werden.

Zu unterscheiden ist immer auch, ob Umstände ein Handeln gebieten oder vielmehr einen Verzicht auf dieses fordern. Da das moral. Gewissen des Menschen nicht in gleichem Maße gewachsen ist wie seine Fähigkeit zu tun (W. JENS), erhebt sich nämlich die Frage, ob im Lichte dieser Einsicht der Mensch nicht schon allein deswegen für die Folgen seines Handelns verantwortlich ist, weil er nicht verzichtet zu tun. Konsequentes Verzichten ist allerdings in einer komplexen und dynam. Welt nicht möglich. Dies befreit die Entscheidungsträger jedoch nicht davon, im Rahmen ihrer historisch gewachsenen Lebenswelt alles Zumutbare zu tun, um von ihren Entscheidungen ausgehende Gefahren zu erkennen und zu berücksichtigen.

→Ethik · Fortschritt · Freiheit · Leben · Risiko · Risikogesellschaft · Schuld · Selbstverwirklichung · Sinn · Technikfolgenabschätzung · Umweltschutz
R. WISSER: V im Wandel der Zeit (1967); W. WEISCHEDEL: Das Wesen der V. (^{3}1972); R. SPAEMANN: Nebenwirkungen als moral. Problem, in: ders.: Zur Kritik der polit. Utopie (1977); WALTER SCHULZ: Philosophie in der veränderten Welt (^{5}1984); H. LENK: Gewissen und V. als Zuschreibungen, in: Ztsch. für philosoph. Forschung, Jg. 41 (1987); Technik und Ethik, hg. v. H. LENK u.a. (1987); K. O. APEL: Diskurs und V. (1988); H. JONAS: Das Prinzip V. (Neuausg. 1989); Verantwortlichkeit und Recht, hg. v. E.-J. LAMPE (1989); N. LUHMANN: Soziologie des Risikos (1991); F.-X. KAUFMANN: Der Ruf Nach V. (1992); V., hg. v. P. FAUSER (1992); O. HÖFFE: Moral als Preis der Moderne (1993).

aus: *Brockhaus Enzyklopädie in 24 Bänden, 19. völlig neu bearbeitete Auflage, 23. Band, Mannheim 1994*

Edward Teller, Atomphysiker, über Politik und Wissenschaft

Matthias Geis: Bloß keine Selbstzweifel; DIE ZEIT Nr. 18, 28. April 1995, Seite 41 (Hervorhebungen durch A. Pfitzmann)

Die Trennung von Wissenschaft und Politik läßt sich nur schwer durchhalten. Seit nunmehr fünfzig Jahren propagiert Edward Teller diese Grenzziehung – und widerlegt sie durch seine Arbeit als Atomphysiker. Machte der Begriff des politischen Naturwissenschaftlers Sinn, Teller wäre sein Prototyp. Der „Vater der Wasserstoffbombe“ hat wie kaum ein anderer Wissenschaftler die Politik für seine Ideen begeistert und mit seinen Erfindungen die Geschichte mitgeprägt. Doch mitverantworten will er sie nicht.

Edward Teller ist zu klug, seine offene politische Einflußnahme – die Durchsetzung der Wasserstoffbombe etwa, später das SDI-Programm – einfach zu dementieren: Er habe sich gelegentlich nicht als Wissenschaftler, sondern als Politiker betätigt und „explizit anders handeln müssen, als ich es für richtig halte“. Doch noch das lockere Eingeständnis ist als Ausnahme formuliert, die die Regel von den separierten Sphären bestätigt.

Wie aber lautet die Regel? Was ist und wo endet die Verantwortung des Wissenschaftlers? Auch im fünfzigsten Jahr nach dem Abwurf der Atombombe über Hiroshima, an deren Entwicklung er

ebenfalls mitwirkte, formuliert Teller wie jüngst in Frankfurt atemberaubend klar und von keinem Zweifel angekränkelt. **Die Pflicht des Wissenschaftlers sei es**, so referierte der 87jährige auf Einladung der Hessischen Stiftung für Frieden und Konfliktforschung, **Wissen zu produzieren und dessen technische Umsetzung zu ermöglichen – „ohne Beschränkung und unter allen Umständen"**. Die konkrete Anwendung und damit die Verantwortung bleibe Sache politischer Entscheidung. Einstein hat am Ende seines Lebens bereut, Roosevelt zum Bau der Bombe bewegt zu haben. Teller: „Ich würde das Bereuen bereuen."

Oppenheimer hat nach Hiroshima von der „Sünde“ der Physiker gesprochen. Teller hat im Gegenzug seine Auffassung einer verantwortungsfreien Wissenschaft radikalisiert: „**Erkenntnisse sind nicht moralischer Natur**“, bescheidet er seine Frankfurter Zuhörer. Verantwortungslos handeln Wissenschaftler für ihn nur dann, wenn sie ihren ureigensten Auftrag, die Wissensproduktion, torpedieren. Wollte man die erkenntnistheoretische Entsprechung zur Wasserstoffbombe formulieren, man käme wohl auf Tellers Credo: „Ich erkenne für die Wissenschaft keine Grenze an.“

Was macht eine Tätigkeit attraktiv, die morgen alles daransetzen wird, ihre giftigen Früchte von heute zu neutralisieren? Fast erscheint es naiv, einem vom Schlage Tellers diese Frage zu stellen. Denn wer die Verantwortung der Forschung auf die Entfesselung des Wissens reduziert, dem gerät auch die Sinnfrage zur wissenschaftsimmanenten Angelegenheit. Die Herausforderung von heute produziert die Herausforderung von morgen.

Teller, der finstere Aufklärer, plaudert mit Humor und Selbstironie. Seinem Publikum verspricht er „klare Antworten“, nicht ohne die Mahnung, alles in zweideutiger Weise aufzunehmen. „In meiner Erfahrung sind die meisten Physiker Dummköpfe. Und in meiner intimen Erfahrung bin ich selbst ein Dummkopf.“ Teller ist ein Kommunikator. Man ahnt, dass seine Überzeugungskraft nicht allein auf Formeln beruht.

Unschuldiger jedenfalls, als Teller es versteht, läßt sich sein unheimliches Wissenschaftsverständnis kaum propagieren: Die Physiker von Los Alamos hätten die Bombe nicht gemacht, sie hätten sie „gefunden“. Vor der „Suche“ und den künftigen „Fundstücken“ solcher Wissenschaft graut es einem. Auch das würde Edward Teller noch ausschließen: „Wir haben kein Recht, Pessimisten zu sein.“

David Lorge Parnas : Die Berufliche Verantwortung von Software-Ingenieuren

Parnas unterscheidet zwischen
- Persönlicher Verantwortung (Personal Responsibility),
- Gesellschaftlicher Verantwortung (Social Responsibility) und
- Beruflicher Verantwortung (Professional Responsibility).

Persönliche Verantwortung trifft alle Personen, egal was ihre Ausbildung oder ihr beruflicher Hintergrund sein mag. Persönliche Verantwortung betrifft grundlegende Pflichten (obligations), wie Ehrlichkeit und Redlichkeit (honesty) im Umgang mit anderen und Berücksichtigung ihres Wohlergehens und ihrer Gefühle.

Berufliche Verantwortung entsteht zusätzlich dadurch, dass wir Mitglieder eines bestimmten Berufsstandes werden, beispielsweise Ärzte, Journalisten oder Ingenieure. Jeder Berufsstand hat für seine Mitglieder Verhaltensregeln entwickelt, die über die allgemeinen persönlichen hinausgehen.

Gesellschaftliche Verantwortung besteht gegenüber der Gesellschaft als Ganzes (im Gegensatz zu Verantwortung gegenüber Individuen). Wer von ihr beispielsweise eine gründliche Ausbildung erhalten hat, sollte dieses Wissen mit der Gesellschaft teilen, wenn es ihr nützen kann.

Viele wichtige Entscheidungen der nächsten Jahrzehnte betreffen technologische Fragen. In unseren demokratischen Gesellschaften werden diese Entscheidungen größtenteils von Nichtwissenschaftlern getroffen. Sie und die Gesellschaft betrachten Wissenschaft oftmals als mystisch, da vollkommen unverständlich, benötigen aber eigentlich verständliche und nachprüfbare Information sowie Rat der Wissenschaftler. Die demokratischen Entscheidungsträger entscheiden aber auch über Wissenschaftsförderung, so dass für Wissenschaftler die Versuchung groß ist, maßlos zu übertreiben (und damit mißzuinformieren), um mehr Forschungsförderung zu erhalten. Folglich müssen WissenschaftlerInnen aus *gesellschaftlicher Verantwortung* einen Teil ihrer Zeit und Energie für die erzieherische Information der Öffentlichkeit aufwenden. Nur wenn eine Entmystifizierung der Wissenschaft gelingt, können informierte Entscheidungen der Regierungen erwartet werden.

> **Ingenieur**: Jemand, der fortgeschrittenes Wissen der Naturwissenschaft, Mathematik und Technik nutzt, um Dinge zu bauen, die andere benutzen.

Software-Engineering hat sich außerhalb der Ingenieursvereinigungen entwickelt.

Berufliche Verantwortung von Software-Ingenieuren:

1. **Individuelle Verantwortlichkeit akzeptieren**: Berufsspezifische (Qualitäts-)Standards haben Vorrang vor Verpflichtungen gegenüber Arbeitgeber oder Kunden. Beispielsweise darf er unangemessene Entwurfsentscheidungen selbst dann nicht billigen, wenn dies dienstlich angeordnet wird.
2. **Das wirkliche Problem lösen**: Sicherstellen, dass das technische Problem, das versucht wird zu lösen, das wirkliche Problem des Auftraggebers ist.
3. **Ehrlichkeit bzgl. der Fähigkeiten**: Für manche Probleme gibt es keine angemessene technische Lösung. Ein Ingenieur hat dies deutlich zu machen und nicht etwa Verträge zu akzeptieren, die ihn anhalten, etwas Unmögliches zu versuchen oder etwas Unmoralisches tun.
4. **Nachvollziehbare Entwürfe**: Entwürfe müssen so dokumentiert und erklärt werden, dass ihre Überprüfung erleichtert wird. Denn Überprüfungen verbessern die Qualität der Produkte.
5. **Wartbarkeit**: Struktur des Produktes und Dokumentation müssen Wartung ermöglichen und erleichtern.

Aus einem Interview mit Intel-Chef Andrew Grove

Ludwig Siegele, Christian Tenbrock: „Die Deutschen haben nicht genug Angst, Ein ZEIT-Gespräch mit Intel-Chef Andrew Grove über die Dominanz des Chipproduzenten und die Technophobie in der Bundesrepublik; DIE ZEIT Nr. 34, 15. August 1997, Seite 17

ZEIT: Sie haben mal gesagt: „Was technologisch möglich ist, wird auch gemacht.” Ist das nicht ein beängstigender Gedanke?

Grove: Schon möglich. Aber er ist wahr. Zeigen Sie mir doch eine Technologie, die nicht gekommen ist, obwohl sie ausgereift und marktfähig war. Man kann Technologie nicht unter Verschluß halten. Sie können nicht bedenklich den Kopf schütteln und sagen: Diese Technologie mag ich nicht. Ein Konkurrent wird sie bestimmt verwenden.

Aufgabe

Setzen Sie sich mit der These „Was technologisch möglich ist, wird auch gemacht.” auseinander.

a) Stimmt sie – oder fallen Ihnen Gegenbeispiele ein.

b) Falls sie nicht stimmt, welche Funktion könnte diese These für diejenigen haben, die sie trotzdem vertreten?

Lösung

a) Die These stimmt zuallermindest in dieser absoluten Formulierung nicht, denn es gibt **Gegenbeispiele**:
   - **Atomenergie**: Diese Technologie wurde nicht nur marktfähig gemacht, sondern auch eingeführt. In vielen Ländern wurde aber beschlossen, aus dieser Technologie wieder auszusteigen oder gar nicht erst einzusteigen.
   - **Solarenergie**: Obwohl ausgereift und marktfähig, verhinderten die großen Stromkonzerne in der Bundesrepublik bis zu einer gesetzlichen Regulierung mittels nicht lukrativer Preise für eingespeisten Strom (verglichen mit bezogenem Strom) einen breiten dezentralen Einsatz.
   - **Magnetschwebebahn**: Obwohl seit vielen Jahren ausgereift und marktfähig, gibt es bisher keinen nennenswerten Einsatz.
   - **Geschlechtsbestimmung von Kindern**: Obwohl seit vielen Jahren zumindest bei Masseneinsatz billige Verfahren zur Geschlechtsbestimmung entwickelt sind und viele Eltern an ihnen Interesse haben, werden diese Verfahren aus Gründe einer wünschenswerten Gleichverteilung der Geschlechter in der Öffentlichkeit weder diskutiert noch gar zum Kauf angeboten.

b) Erstens hat die These die Funktion, von Verantwortung zu entlasten, etwa in dem Sinne: Wenn dies Unerwünschte/Schädliche/Ambivalente etc. sowieso kommt, dann brauchen wir nicht darüber nachzudenken, ob wir's einführen und vermarkten dürfen und wollen. Zweitens hat die These die Funktion, anderen zu suggerieren, sie hätten keine Wahl. Die These dient also der Interessendurchsetzung der Technologie-Entwickler und -Vermarkter.

Berufsethos, Berufsethik, Berufsrecht, Hippokratischer Eid für InformatikerInnen?

Jede Berufsvereinigung ist eine Konspiration gegen die Öffentlichkeit.
Max Weber
zitiert nach: Erwin K. Scheuch: Ein schlechtes Kursbuch; FAZ Feuilleton vom 21. Feb. 1990;
nachgedruckt in UNIFAZ Folge 34, Sommersemester 1990, Seite 20

Hier wird nur eine kleine Auswahl von Originaltexten von Kodizes vorgestellt. Weitere Kodizes, einige Übersetzungen sowie inhaltliche Zusammenfassungen sind im Anhang des Skripts zu finden.

ACM Code of Professional Conduct and Procedure for the Enforcement of the ACM Code of Professional Conduct (Association for Computing Machinery, 1972)

zitiert nach [IFIP_92 = IFIP-WG9.2 On Behalf of IFIP-TC9: Ethics of Computing: Information Technology and Responsibility; To Promote Discussion Inside the IFIP National Societies; Madrid, september 1992]

Preamble:
Recognition of professional status by the public depends not only on skill and dedication but also on adherence to a recognized Code of Professional Conduct. The following Code sets forth the general principles (Canon) followed by professional ideals (Ethical Considerations), and mandatory rules (Disciplinary Rules) applicable to each ACM Member.

The verbs "shall" (imperative) and "should" (encouragement) are used purposefully in the Code. The Canons and Ethical Considerations are not, however, binding rules. Each Disciplinary Rule is binding on each individual Member of ACM. Failure to observe the Disciplinary Rules subjects the Member to admonition, suspension or expulsion from the Association as provided by the Procedures for the Enforcement of the ACM Code of Professional Conduct, which are specified in the ACM Policy and Procedures Guidelines. The term "member(s)" is used in the Code. The Disciplinary Rules of the Code apply, however, only to the classes of membership specified in Article 3, Section 4, of the Constitution of the ACM.

An ACM member:

Canon 1. Act at all times with integrity:
EC1.1. ... shall properly qualify himself when expressing an opinion outside his areas of competence.
EC1.2. ... shall preface any partisan statement about information processing by indication clearly on whose behalf they are made.
EC1.3. ... shall act faithfully on behalf of his employers or clients.

Canon 2. Strive to increase his competence and the competence and prestige of the profession:

EC2.1. ... is encouraged to extend public knowledge, understanding, and appreciation of information processing, and to oppose any false or deceptive statements relating to information processing of which he is aware.
EC2.2. ... shall not use his professional credentials to misrepresent his competence.
EC2.3. ... shall undertake only those professional assignments and commitments for which he is qualified.
EC2.4. ... shall strive to design and develop systems that adequately perform the intended functions and that satisfy his employer's or client's operational needs.
EC2.5. ... should maintain and increase his competence through a program of continuing education encompassing the techniques, technical standards, and practices in his fields of professional activity.
EC2.6. ... should provide opportunity and encouragement for professional development and advancement of both professionals and those aspiring to become professionals.

Canon 3. Accept responsibility for his work:
EC3.1. ... shall accept only those assignments for which there is reasonable expectancy of meeting requirements or specifications, and shall perform his assignments in a professional manner.

Canon 4. Act with professional responsibility:
EC4.1. ... shall not use his membership in ACM improperly for professional advantage or to misrepresent the authority of his statements.
EC4.2. ... shall conduct professional activities on a high plane.
EC4.3. ... is encouraged to uphold and improve the professional standards of the Association through participation in their formulation, establishment, and enforcement.

Canon 5. Use his special knowledge and skills for the advancement of human welfare:
EC5.1. ... should consider health, privacy, and general welfare of the public in the performance of his work.
EC5.2. ... whenever dealing with data concerning individuals, shall always consider the principle of the individual's privacy and seek the following:

To minimize the data collected,
To limit authorized access to the data,
To provide proper security for the data,
To determine the required retention period of the data,
To ensure proper disposal of the data.

ACM Code of Ethics and Professional Conduct

October 16, 1992 (veröffentlicht in Communications of the ACM 36/2 (1993) 99ff.)

Commitment to ethical professional conduct is expected of every voting, associate, and student member of ACM. This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment.

It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity, for example with organizations such as ACM. Principles involving compliance with this Code are given in Section 4.

The Code is supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that Guidelines will be changed more frequently than the Code.

The Code and its supplemented guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the moral imperatives section, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. General Moral Imperatives

(As an ACM member I will...)

1.1 Contribute to society and human well-being
1.2 Avoid harm to others
1.3 Be honest and trustworthy
1.4 Be fair and take action not to discriminate
1.5 Honor property rights including copyrights and patents
1.6 Give proper credit for intellectual property
1.7 Respect the privacy of others
1.8 Honor confidentiality

2. More Specific Professional Responsibilities

(As an ACM computing professional I will...)

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work
2.2 Acquire and maintain professional competence
2.3 Know and respect existing laws pertaining to professional work
2.4 Accept and provide appropriate professional review
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks
2.6 Honor contracts, agreements, and assigned responsibilities
2.7 Improve public understanding of computing and its consequences
2.8 Access computing and communication resources only when authorized to do so

3. Organizational Leadership Imperatives

(As an ACM member and an organizational leader, I will...)

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities
3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life
3.3 Acknowledge and support proper and authorized uses of an organization's computing and communications resources

3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements. Later the system must be validated to meet requirements.
3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system
3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems

4. Compliance with the Code
(As an ACM member I will...)
4.1 Uphold and promote the principles of this Code
4.2 Treat violations of this code as inconsistent with membership in the ACM

In der angegebenen Quelle sind einerseits zu jedem moralischen Imperativ längere Erläuterungen enthalten und andererseits Beispielfälle im begleitenden Artikel: [AJGP_93 = Ronald E. Anderson, Deborah G. Johnson, Donald Gotterbarn, Judith Perrolle: Using the ACM Code of Ethics in Decision Making; Communications of the ACM 36/2 (1993) 98-107].

Ethische Leitlinien der Gesellschaft für Informatik e.V.

http://www.gi-ev.de/verein/struktur/index-ethik.html

Die Leitlinien wurden am 13.01.1994 vom Präsidium der GI verabschiedet und am 16.12.1994 von den Mitgliedern bestätigt (diese Fassung ist im Anhang enthalten). Am 29. Januar 2004 hat das GI-Präsidium die Ethischen Leitlinien in einer komplett überarbeiteten Version angenommen.

Ausgearbeitet vom Arbeitskreis "Verantwortung" der GI:
Peter Bittner, Rafael Capurro, Wolfgang Coy, Eva Hornecker, Constanze Kurz, Karl-Heinz Rödiger (Sprecher), Britta Schinzel, Ute Twisselmann, Roland Vollmar, Karsten Weber, Alfred Winter, Cornelia Winter

Präambel

Das Handeln von Informatikerinnen und Informatikern steht in Wechselwirkung mit unterschiedlichen Lebensweisen, deren besondere Art und Vielfalt sie berücksichtigen sollen. Mehr noch sehen sie sich dazu verpflichtet, allgemeine moralische Prinzipien, wie sie in der Allgemeinen Deklaration der Menschenrechte formuliert sind, zu wahren. Diese Leitlinien sind Ausdruck des gemeinsamen Willens, diese Wechselwirkungen als wesentlichen Teil des eigenen individuellen und institutionellen beruflichen Handelns zu betrachten. Der offene Charakter der nachfolgenden Artikel wird mit dem Begriff Leitlinien unterstrichen.

Die Gesellschaft für Informatik (GI) will mit diesen Leitlinien bewirken, dass berufsethische Konflikte Gegenstand gemeinsamen Nachdenkens und Handelns werden. Ihr Interesse ist es, ihre Mitglieder, die sich mit verantwortungsvollem Handeln exponiert haben, zu unterstützen. Vor allem will sie den Diskurs über ethische Fragen in der Informatik mit der Öffentlichkeit aufnehmen und Aufklärung leisten.

Handlungsalternativen und ihre absehbaren Wirkungen fachübergreifend zu thematisieren, ist in einer vernetzten Welt eine notwendige Aufgabe; hiermit sind Einzelne zumeist überfordert. Deshalb hält es die GI für unerlässlich, die Zusammenhänge zwischen individueller und gemeinschaftlicher

Verantwortung zu verdeutlichen und dafür Verfahren zu entwickeln. Im Sinne dieser Ausführungen bindet sich die GI an die folgenden Leitlinien. Die ethischen Leitlinien werden regelmäßig überarbeitet.

Viele Forderungen sind dabei solche nach Professionalität, denen sich angestellte und selbstständige Informatikerinnen und Informatiker gleichermaßen stellen müssen. Kompetenz in der Ausübung des Berufs ist zwar selbst noch kein moralisches Handeln, doch ist die bewusste Hinnahme fehlender Fähigkeiten verantwortungslos. Professionalität ermöglicht in diesem Sinne verantwortungsvolles Handeln; sie ist Bedingung dafür, dass das berufliche Handeln den Rechten der Betroffenen gerecht werden kann.

I. Das Mitglied

Art. 1 - FACHKOMPETENZ
Vom Mitglied wird erwartet, dass es seine Fachkompetenz nach dem Stand von Wissenschaft und Technik ständig verbessert.

Art. 2 - SACHKOMPETENZ UND KOMMUNIKATIVE KOMPETENZ
Vom Mitglied wird erwartet, dass es seine Fachkompetenz hin zu einer Sach- und kommunikativen Kompetenz erweitert, sodass es die seine Aufgaben betreffenden Anforderungen an die Datenverarbeitung und ihre fachlichen Zusammenhänge versteht sowie die Auswirkungen von Informatiksystemen im Anwendungsumfeld beurteilen und geeignete Lösungen vorschlagen kann. Dazu bedarf es der Bereitschaft, die Rechte und Interessen der verschiedenen Betroffenen zu verstehen und zu berücksichtigen. Dies setzt die Fähigkeit und Bereitschaft voraus, an interdisziplinären Diskussionen mitzuwirken und diese gegebenenfalls aktiv zu gestalten.

Art. 3 - JURISTISCHE KOMPETENZ
Vom Mitglied wird erwartet, dass es die einschlägigen rechtlichen Regelungen kennt, einhält und gegebenenfalls an ihrer Fortschreibung mitwirkt.

Art. 4 - URTEILSFÄHIGKEIT
Vom Mitglied wird erwartet, dass es seine Urteilsfähigkeit entwickelt, um als Informatikerin oder Informatiker an Gestaltungsprozessen in individueller und gemeinschaftlicher Verantwortung mitwirken zu können. Dies setzt die Bereitschaft voraus, das eigene und das gemeinschaftliche Handeln in Beziehung zu gesellschaftlichen Fragestellungen zu setzen und zu bewerten. Es wird erwartet, dass allgemeine moralische Forderungen beachtet werden und in Entscheidungen einfließen.

II. Das Mitglied in einer Führungsposition

Art. 5 - ARBEITSBEDINGUNGEN
Vom Mitglied in einer Führungsposition wird zusätzlich erwartet, dass es für Arbeitsbedingungen und Weiterbildungsmöglichkeiten Sorge trägt, die es Informatikerinnen und Informatikern erlauben, ihre Aufgaben nach dem Stand der Technik auszuführen und die Arbeitsergebnisse zu evaluieren.

Art. 6 - ORGANISATIONSSTRUKTUREN
Vom Mitglied in einer Führungsposition wird zusätzlich erwartet, aktiv für Organisationsstrukturen und Möglichkeiten zur Diskussion einzutreten, die die Übernahme individueller und gemeinschaftlicher Verantwortung ermöglichen.

Art. 7 - BETEILIGUNG
Vom Mitglied in einer Führungsposition wird zusätzlich erwartet, dass es dazu beiträgt, die von der Einführung von Informatiksystemen Betroffenen an der Gestaltung der Systeme und ihrer Nutzungsbedingungen angemessen zu beteiligen. Von ihm wird insbesondere erwartet, dass es

keine Kontroll- und Überwachungstechniken ohne Unterrichtung und Beteiligung der Betroffenen zulässt.

III. Das Mitglied in Lehre und Forschung

Art. 8 - LEHRE
Vom Mitglied, das Informatik lehrt, wird zusätzlich erwartet, dass es die Lernenden auf deren individuelle und gemeinschaftliche Verantwortung vorbereitet und selbst hierbei Vorbild ist.

Art. 9 - FORSCHUNG
Vom Mitglied, das auf dem Gebiet der Informatik forscht, wird zusätzlich erwartet, dass es im Forschungsprozess die allgemeinen Regeln des guten wissenschaftlichen Arbeitens einhält. Dazu gehören insbesondere Offenheit und Transparenz, Fähigkeit zur Äußerung und Akzeptanz von Kritik sowie die Bereitschaft, die Auswirkungen der eigenen wissenschaftlichen Arbeit im Forschungsprozess zu thematisieren.

VI. Die Gesellschaft für Informatik

Art. 10 - ZIVILCOURAGE
Die GI ermutigt ihre Mitglieder in Situationen, in denen ihre Pflichten gegenüber Arbeitgebern oder Kundenorganisationen in Konflikt mit der Verantwortung gegenüber anderweitig Betroffenen stehen, mit Zivilcourage zu handeln.

Art. 11 - SOZIALE VERANTWORTUNG
Die GI unterstützt den Einsatz von Informatiksystemen zur Verbesserung der lokalen und globalen Lebensbedingungen. Informatikerinnen und Informatiker tragen Verantwortung für die sozialen und gesellschaftlichen Auswirkungen ihrer Arbeit; sie sollen durch ihren Einfluss auf die Positionierung, Vermarktung und Weiterentwicklung von Informatiksystemen zu ihrer sozial verträglichen Verwendung beitragen.

Art. 12 - MEDIATION
Die GI übernimmt Vermittlungsfunktionen, wenn Beteiligte in Konfliktsituationen diesen Wunsch an sie herantragen.

Art. 13 - INTERDISZIPLINÄRE DISKURSE
Die GI initiiert und fördert interdisziplinäre Diskurse zu ethischen und sozialen Problemen der Informatik; deren Ergebnisse werden veröffentlicht.

Erläuterungen der Begriffe

Diskurs

Diskurse sind Verfahren gemeinschaftlicher Reflexion von Problemen mit einem normativen, wertbezogenen Hintergrund, die von Einzelnen oder einer einzelnen Fachdisziplin nicht überschaut werden können. Ihre wesentliche Leistung liegt darin, in der fachübergreifenden Kommunikation Erkenntnis- und Verständnisgrenzen zu überwinden sowie Vor-Urteile zu hinterfragen und im Lichte anderer Positionen zu überprüfen.

Gesellschaftliche Auswirkungen

Gesellschaftliche Auswirkungen moderner Informations- und Kommunikationstechnologie umfassen beispielsweise die digitale Kluft (engl. „digital divide“), veränderte Arbeitsstrukturen in Betrieben, Rationalisierung und Schaffung neuer Arbeitsplätze, verändertes Kommunikations- und Sozialverhalten, die Entstehung virtueller Gemeinschaften etc.

Gutes wissenschaftliches Arbeiten

Infolge der Aufdeckung schwerwiegenden Fehlverhaltens wie Betrug, Fälschung oder Plagiate wurden beispielsweise von der Max-Planck-Gesellschaft Regeln des guten wissenschaftlichen Arbeitens formuliert. Darin wird unter anderem gefordert, dass Wissenschaftlerinnen und Wissenschaftler Hypothesen systematisch prüfen und keine Informationen unterschlagen, die gegen eigene Hypothesen sprechen; die Prüfung von Hypothesen muss dem jeweils anerkannten Forschungsstand folgen; Wissenschaftlerinnen und Wissenschaftler sollen in diesem Prozess neutral und objektiv agieren. Die Befolgung dieser Normen beinhaltet selbstverständlich auch, dass Wissenschaftlerinnen und Wissenschaftler weder Fälschungen oder Plagiate benutzen, um eigene Forschungsergebnisse zu produzieren bzw. zu stützen, noch auf andere Weise versuchen, die jeweilige wissenschaftliche Gemeinde zu täuschen.

Informatiksystem

Unter einem Informatiksystem wird die Einheit von Hardware, Software und Netzen und aller durch sie intendierten oder verursachten Gestaltungs- und Qualifizierungsprozesse bezüglich Arbeit und Organisation verstanden.

Kontroll- und Überwachungstechniken

Unter Kontroll- und Überwachungstechnik werden analog zum Betriebsverfassungsgesetz „technische Einrichtungen“ verstanden, die objektiv geeignet sind, „das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ (§ 87 Abs. 1 Nr. 6 BetrVG). Bei Einführung und Betrieb solcher Systeme steht den Interessenvertretungen ein Mitbestimmungsrecht zu. Alle von Kontroll- und Überwachungstechniken Betroffenen haben das Recht auf informationelle Selbstbestimmung.

Mediation

Unter Mediation werden Verhandlungsprozesse verstanden, mit deren Hilfe Interessenkonflikte zwischen zwei oder mehreren Parteien unter Hinzuziehung eines neutralen Dritten (Mediator) beigelegt werden. Das Ziel sind Problemlösungen, die von allen am Prozess Beteiligten akzeptiert werden. Der Mediationsprozess ist durch das Ausloten von Handlungsspielräumen und durch die Suche nach neuen Lösungen gekennzeichnet. Die Ergebnisse sind nicht rechtlich verpflichtend; als erfolgreich erweisen sich allgemein „Jeder-gewinnt- Lösungen“.

Rechtliche Regelungen

Rechtliche Regelungen, die für die Gestaltung von Informatiksystemen bedeutsam sind, finden sich inzwischen in nahezu allen Bereichen der Rechtsordnung.

Ohne eine Rangfolge anzudeuten, zählen dazu insbesondere: Datenschutzrecht: Allgemeiner und bereichsspezifischer Datenschutz, einschließlich Arbeitnehmerdatenschutz; Freedom-of-information-Gesetzgebung (Informationszugangsgesetze, z.B. für den Umweltbereich); Computerstrafrecht; Gewerblicher Rechtsschutz, Urheber- und Patentrecht, Markenrecht; Recht der Produkthaftung; Recht zur IT-Sicherheit (SigG, SigV, BSIG); Telekommunikationsrecht; Medienrecht; Jugendschutzrecht; Verbraucherschutzrecht.

In vielen, bei weitem aber nicht in allen Fällen begründet die Einhaltung technischer Normen und Standards (DIN, EN, ISO) die Vermutung der Rechtstreue.

Stand von Wissenschaft und Technik

Die Leitlinien wären schon bei ihrer Verkündung veraltet, wenn man sie auf einen schon bekannten Wissensfundus in der Informatik bezöge. Statt starrer Verweise bietet sich als Ausweg an, das Prinzip der sogenannten offenen normativen Standards zu übernehmen, für das sich das deutsche technische Sicherheitsrecht entschieden hat. Das Bundesverfassungsgericht hat dieses Prinzip in mehreren Grundsatzentscheidungen zu einer sogenannten „Dreistufenlehre“ konkretisiert (BVerfGE 49, 89 ff., BVerfGE 53, 30 ff., BVerfGE 56, 54 ff.):

1. Stufe: Allgemein anerkannte Regeln der Technik
Eine Regel ist dann allgemein anerkannt, wenn die herrschende Meinung der Praktiker eines Fachgebiets von ihrer Richtigkeit überzeugt ist und dies auch dokumentiert hat. Die Regel muss in der Fachpraxis bewährt und erprobt sein. Maßgebend ist die Durchschnittsmeinung der Praktiker, abweichende Auffassungen von Minderheiten sind unerheblich. Eine starke faktische Vermutung für die allgemeine Anerkennung besteht, wenn zum Beispiel DIN oder ISO-Normen für das Problem existieren.

2. Stufe: Stand der Technik
Der Maßstab für das Gebotene wird an die Front der technischen Entwicklung verlagert, für die die allgemeine Anerkennung und die praktische Bewährung alleine nicht ausreichen. Bei dieser Formel müssen Meinungsverschiedenheiten unter technischen Praktikern ermittelt werden. Die meisten Datenschutzgesetze enthalten in ihren Datensicherungsvorschriften einen Hinweis auf den „Stand der Technik (und Organisation)“.

3. Stufe: Stand von Wissenschaft und Technik
Mit der Bezugnahme auf diese Formel wird ein noch stärkerer Zwang dahin ausgeübt, dass eine Regel mit der wissenschaftlichen und technischen Entwicklung Schritt hält. Geboten ist, was nach neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird. Das jeweils Erforderliche wird also nicht durch das technisch gegenwärtig Machbare begrenzt. Einen Verweis auf den „Stand von Wissenschaft und Technik“ enthält zum Beispiel das Produkthaftungsgesetz von 2002, das zumindest für Standardsoftware anwendbar ist.

Es bietet sich an, an die Fachkompetenz der Informatikerinnen und Informatiker besonders hohe Maßstäbe anzulegen (3. Stufe). Bei der Realisierung von Informatiksystemen müsste es im Allgemeinen ausreichen, die Erwartungen, wie sie zum Beispiel Datenschutzgesetze an Informatikerinnen und Informatiker haben, jedenfalls nicht zu unterschreiten.

Verantwortung

1. Individuell

Ethik befasst sich mit dem vorbedachten Handeln von Menschen, die die Folgen ihres Handelns für andere Menschen, ihre Mitgeschöpfe und die Umwelt reflektieren. Hierbei können die Folgen des Handelns unmittelbar oder über längere Zeiten und größere Räume zu bedenken sein. Was der einzelne Mensch hinsichtlich dieser Handlungsfolgen und der moralischen Bewertung der Handlung selbst bedenken und beeinflussen kann, obliegt seiner individuellen Verantwortung. Eine Definition von Verantwortung beinhaltet mindestens folgende Komponenten:

jemand ist verantwortlich	» Personen, Korporationen etc.
für *etwas*	» Folgen
gegenüber einem *Adressaten*	» Betroffene
vor *einer Instanz*	» Sanktions- und/oder Urteilsinstanzen
in Bezug auf *Kriterien*	» Normen, Werte
im Rahmen *eines bestimmten Kontextes*	» Verantwortungs- und/oder Handlungsbereiche

Da Menschen die Folgen ihres Handelns nicht immer abschätzen können, sollten Entscheidungen stets so getroffen werden, dass sie widerrufbar sind und korrigierbar bleiben. Damit wird der Handlungsspielraum aller Beteiligten erweitert und nicht von vornherein alternativlos eingeschränkt.

2. Gemeinschaftlich

Für den einzelnen Menschen sind die Folgen gemeinschaftlichen Handelns in Organisationen, Gruppen, Wirtschaften und Kulturen nicht immer überschaubar. Gemeinschaftliches Handeln bedarf deshalb zusätzlich zur individuellen der gemeinschaftlichen Reflexion. Gemeinschaftliche Verantwortung beruht auf der Möglichkeit, mit Vor-Sicht künftige Handlungen, die sich nicht oder nur teilweise an Erfahrungen und daraus entwickelten Normen orientieren können, gemeinschaftlich zu bedenken. Eine besondere Notwendigkeit solcher Reflexion ergibt sich immer dann, wenn individuelle Ansprüche mit jenen einer Gemeinschaft in Konflikt geraten, die Handlungsmöglichkeiten einzelner Personen nicht ausreichen oder eindeutige Verantwortungszuweisungen nicht möglich sind. Diskurse sind mögliche Verfahren der gemeinschaftlichen Reflexion über Verantwortungsfragen.

Software Engineering Code of Ethics and Professional Practice

(Version 5.2) as recommended by the
IEEE-CS/ACM Joint Task Force on Software Engineering Ethics and Professional Practices and jointly approved by the ACM in Nov. 1998 and the IEEE-CS in Dec. 1998 as the standard for teaching and practicing software engineering.

Short Version

PREAMBLE

The short version of the code summarizes aspirations at a high level of abstraction. The clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1 PUBLIC - Software engineers shall act consistently with the public interest.

2 CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest.

3 PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4 JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.

5 MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

6 PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7 COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.

8 SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Full Version

PREAMBLE

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and in the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations, standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the "Public Interest" is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

PRINCIPLES

Principle 1 PUBLIC Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01. Accept full responsibility for their own work.

1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07. Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.

1.08. Be encouraged to volunteer professional skills to good causes and to contribute to public education concerning the discipline.

Principle 2 CLIENT AND EMPLOYER Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02. Not knowingly use software that is obtained or retained either illegally or unethically.

2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.

2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08. Accept no outside work detrimental to the work they perform for their primary employer.

2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

Principle 3 PRODUCT Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01. Strive for high quality, acceptable cost, and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.

3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04. Ensure that they are qualified for any project on which they work or propose to work, by an appropriate combination of education, training, and experience.

3.05. Ensure that an appropriate method is used for any project on which they work or propose to work.

3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

3.07. Strive to fully understand the specifications for software on which they work.

3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users requirements and have the appropriate approvals.

3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.

3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

Principle 4 JUDGMENT Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01. Temper all technical judgments by the need to support and maintain human values.

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

Principle 5 MANAGEMENT Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance. In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02. Ensure that software engineers are informed of standards before being held to them.

5.03. Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.

5.07. Offer fair and just remuneration.

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11. Not ask a software engineer to do anything inconsistent with this Code.

5.12. Not punish anyone for expressing ethical concerns about a project.

Principle 6 PROFESSION Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01. Help develop an organizational environment favorable to acting ethically.

6.02. Promote public knowledge of software engineering.

6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04. Support, as members of a profession, other software engineers striving to follow this Code.

6.05. Not promote their own interest at the expense of the profession, client or employer.

6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10. Avoid associations with businesses and organizations which are in conflict with this code.

6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13. Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

Principle 7 COLLEAGUES Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly-documented way.

7.05. Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

Principle 8 SELF Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06 Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

This Code was developed by the IEEE-CS/ACM joint task force on Software Engineering Ethics and Professional Practices (SEEPP):

Executive Committee: Donald Gotterbarn (Chair),

Keith Miller and Simon Rogerson;

Members: Steve Barber, Peter Barnes, Ilene Burnstein, Michael Davis, Amr El-Kadi, N. Ben Fairweather, Milton Fulghum, N. Jayaram, Tom Jewett, Mark Kanko, Ernie Kallman, Duncan Langford, Joyce Currie Little, Ed Mechler, Manuel J. Norman, Douglas Phillips, Peter Ron Prinzivalli, Patrick Sullivan, John Weckert, Vivian Weil, S. Weisband and Laurie Honour Werth.

`http://www-cs.etsu.edu/seeri/secode.htm`

Einen sehr kritischen Leserbrief von David Lorge Parnas zu diesem Kodex und eine Antwort darauf von Don Gotterbarn, Keith Miller und Simon Rogerson finden Sie in Software Engineering Notes 24/3 (May 1999) 4-6.

Was fällt auf?

Während der älteste mir bekannte Ethische Kodex für Informatiker (ACM, 1972) noch durchgehend nur an das *Individuum* appelliert und fast ausschließlich nur *individuelle Aktivitäten* betrachtet (mit der Ausnahme von EC4.3, wo immerhin ein kollektiver Prozeß angesprochen wird – auch wenn es sich nur um Binnenaktivität innerhalb der "Association" handelt), widmet der 20 Jahre jüngere ACM Kodex von 1992 *kollektiven Aktivitäten*, wenn auch nur innerhalb einer Hierarchie, immerhin ein ganzes Viertel des Textes ("Organizational Leadership Imperatives") und der ACM/IEEE Software Engineering Code von 1998 den 5. von 8 Teilen sowie immerhin noch die Unterpunkte 6.10 und 8.08. Noch deutlich weiter gehen hier die Ethischen Leitlinien der GI von 1994, in denen explizit nicht nur von *individueller*, sondern auch *kollektiver Ethik* geredet wird. Hier werden in Abschnitt IV erstmals auch (kollektive moralische) Verpflichtungen der Berufsvereinigung explizit gemacht: „Die GI ...“. Was der Betroffene im Einzelfall davon hat (geht z.B. die Ermunterung von Art. 9 soweit, dass jemand, der wegen Zivilcourage gegenüber seinem Arbeitgeber von diesem gefeuert wurde, auch finanzielle Unterstützung vom Kollektiv, sprich der GI, erhält – oder soll er dann von Luft und Liebe sowie Ermutigung leben?) bleibt offen. Aber immerhin – dies ist ein Anfang!

Die ethischen Imperative sind ziemlich allgemein gültig, nahezu nichts ist Informatik-spezifisch. Es stellen sich da kanonischerweise zwei Gruppen von Fragen:

1. Wozu die Aufzählung allgemeiner ethischer Imperative? Was bezweckt eine Berufsvereinigung damit? Ist es nötig und sinnvoll, zu fordern und zu verkünden: Wir alle wollen/sollen/sind redliche und verantwortungsvolle Menschen? (vgl. unten: Härteste mir bekannte Kritik an der Idee "Code of Professional Ethics")
2. Gibt es Informatik-spezifische Fragen? Wenn ja, weshalb drücken sich die vier ethischen Kodizes vor ihnen? (vgl. unten: Zur Verantwortung der Informatiker)

Härteste mir bekannte Kritik an der Idee "Code of Professional Ethics"

John Ladd: The Quest for a Code of Professional Ethics: An Intellectual and Moral Confusion; in: D. G. Johnson, J. W. Snapper: Ethical Issues in the Use of Computers; Belmont, Wadsworth 1985, 8-13.

Zur Begrifflichkeit: Ethik ist eine niemals endende, reflektierende und kritische Aktivität. Ethische Prinzipien können nur durch (persönliche) Abwägung und Argumentation herausgefunden werden. Ethische Prinzipien können nicht wie Gesetze, Regeln oder Ziele durch Autorität verordnet oder vereinbart werden. Deshalb können ethische Prinzipien nicht durch Vereinigungen, Organisationen und auch nicht durch Konsens ihrer Mitglieder errichtet werden.

Ethik setzt voraus, dass Personen autonom moralisch agieren. Deshalb müssen ethische Forderungen vom Menschen an sich selbst statt an andere gerichtet werden.

Oftmals wird „ethisch“ im Sinne von „nicht durch Gesetz vorgeschrieben“ verwendet.

Ethik kann allerdings zur Beurteilung eines disziplinierenden Kodex (disciplinary code), straf(recht)lichen Kodex (penal code) oder Ehrenkodex (code of honor) – oder was immer unter einem ethischen Kodex (code of ethics) verstanden werden mag – dienen.

Kodizes richten sich oftmals nicht an die Mitglieder der die Kodizes habenden Vereinigungen oder Organisationen, sondern an andere Adressaten, die etwa beeindruckt, in Ruhe gewiegt etc. werden sollen.

Kodizes können dazu dienen, das Monopole einer Vereinigung oder Organisation zu schützen.

Kodex-konformes Verhalten, so unethisch es auch immer sein mag, kann als „ethisch“ gerechtfertigt werden.

Kodizes lenken von der makro-ethischen Sicht ab und rücken mikro-ethische Gesichtspunkte ins Zentrum. Hierbei werden unter **makro-ethischen** Problemen kollektive oder soziale Probleme verstanden, also solche, die die Mitglieder eines Berufsstandes *als Gruppe* in Bezug auf die Gesellschaft betreffen. **Mikro-Ethik** betrifft moralische Aspekte *persönlicher* Beziehungen zwischen individuellen Mitgliedern eines Berufsstandes und andern Individuen, etwa ihren Kunden, Kollegen oder Arbeitgebern.

Kodizes können zur Willkürherrschaft der Mehrheit oder gar nur des Establishment einer Vereinigung oder Organisation über Mitglieder mit abweichender Meinung, innovativen Ideen oder Kritik dienen.

Zur Verantwortung der Informatiker*

Andreas Pfitzmann, Universität Hildesheim, Institut für Informatik, W-3200 Hildesheim

Zusammenfassung

Es wird motiviert und gefordert, präzise zu dokumentieren, wer bei der Konstruktion von informationstechnischen Systemen wofür verantwortlich ist. Dies könnte das Spezifische eines zu schaffenden Berufsrechts für Informatiker sein.

1 Motivation

Wir alle wissen, dass Menschen hin und wieder Fehler machen. Die heutigen informationstechnischen Systeme (IT-Systeme) sind vermutlich einerseits die

- kompliziertesten von Menschen geschaffenen Systeme[34], andererseits die
- am freiesten von Menschen geschaffenen, vgl. Kapitel 2.

Ersteres sollte uns davor warnen, ihnen blind zu vertrauen, denn je komplizierter etwas ist, desto größer ist die Wahrscheinlichkeit, dass darin Fehler enthalten sind.

Letzteres fordert uns heraus. Denn die vorhandene Freiheit sollte es uns erlauben, IT-Systeme so zu strukturieren, dass sie aus wohlverstandenen, oft geprüften Teilen wohlverstanden zusammengesetzt werden. Dann wäre der bereits heute zu beobachtende Einsatz von Informationstechnik auch in kritischen Bereichen zumindest technisch zu rechtfertigen. Leider wird es dazu nötig sein, auf zumindest manche Zusammensetzungsprinzipien und Konstruktionstechniken zu vertrauen. In ihnen müssen Fehler unbedingt vermieden werden, etwa indem jedes kritische Programm von sehr vielen gelesen und testiert wird.

Deshalb plädiere ich im folgenden, nicht aus „Irren ist menschlich“ auf „Entwurfsfehler machen ist keine Schande“ zu schließen und dies zu „Noch besser ist unklar zu lassen, was überhaupt ein Fehler ist und wo ggf. er steckt und wer ihn verbrochen hat“ zu steigern. Ich befürworte im folgenden eine möglichst präzise Dokumentation, wer bei der Konstruktion eines IT-Systems wofür verantwortlich ist.

Zumindest manche mit der Konstruktion von IT-Systemen Beschäftigte werden eine solche präzise Dokumentation nicht *wollen*, da viele[35] Menschen lieber nicht kontrollierbar arbeiten und ungern

---

* Erschien im Datenschutz-Berater 15/8-9 (Aug. 1991) 2-7; Literaturhinweise wurden für den Nachdruck in INFORMATIK FORUM, Band 7, Nr. 1-2, März/Juni 1993, ISSN 1010-6111, Wien sowie später für diese Vorlesungsnotizen aktualisiert. Die Fußnoten in diesen 1991 geschriebenen Text habe ich 1996 eingefügt, nachdem mir (von lieben FreundInnen) klar (gemacht) wurde, dass dieser Text zumindest in Teilen sehr problematisch ist. Die Fußnoten mögen sowohl zur Kompensation wie auch zur Belustigung dienen ...

[34] Dies ist, so wie geschrieben, blühender Blödsinn: Kinder oder auch soziale Gemeinschaften sind deutlich komplizierter ... Da bin ich wohl der typischen Technikersicht selbst aufgesessen: Es wird nur die technische Welt gesehen ... Allenfalls gilt also: ... die kompliziertesten von Menschen geschaffenen *technischen* Systeme...

Fehler zugeben. Außerdem gibt es chaotisch strukturierte IT-Systeme, wo man diese präzise Dokumentation beim besten Willen im nachhinein nicht erreichen *kann*. Sicherlich gibt es auch Aufgabenstellungen, wo präzise Dokumentation, wer bei der Konstruktion eines IT-Systems wofür verantwortlich ist, beim heutigen Stand der Kunst auch bei geeigneter Strukturierung des IT-Systems nicht befriedigend erreichbar ist. All dies stellt aus meiner Sicht hauptsächlich die betroffene Anwendung der Informationstechnik in Frage und nicht meinen Vorschlag.

2 Das Spezifische der Informatik

Im Gegensatz zu den Natur- bzw. Ingenieurwissenschaften hat der Informatiker nicht primär die *vorgegebene* materielle Natur zu erforschen bzw. gegen die Widerspenstigkeit und Knappheit von Materie und Rohmaterialien anzukämpfen. Der Informatiker kann, von materiellen Grenzen wie Entfernung, Reibung, Verschleiß und Alterung durch den informationstechnischen Fortschritt zunehmend befreit, seine informationstechnischen Systeme fast beliebig *gestalten* oder auch *wuchern lassen*. Neben der für die meisten praktischen Anwendungen irrelevanten „naturgegebenen“ Beschränkung auf das überhaupt genügend effizient Berechenbare und der durch menschliche Organisationsformen gegebenen Beschränkung bzgl. Zeit, Personal und Geld erlebt der Informatiker als Begrenzung – zugespitzt: Gegner – hauptsächlich seine eigenen begrenzten gedanklichen Fähigkeiten. Zusätzlich setzen in der Praxis mangelnde Motivation, Konzentration und Sorgfalt noch engere Grenzen.

Da die meisten Menschen ungern persönliches Versagen erleben oder gar zugeben und da bei IT-Systemen ein Abschieben auf vorgegebene äußere Naturgesetze und begrenzte materielle Ressourcen meist nicht möglich ist, lassen die meisten Menschen – teils unbewußt – die genaue Urheberschaft und folglich auch die Verantwortung für IT-Systeme heute weitgehend unklar. Beispielsweise ist einem Programm weder anzusehen noch bisher technisch zugeordnet, wer was entworfen, programmiert oder geändert hat und welche Annahmen dabei jeweils über die Umgebung des Programms (andere, insbesondere aufgerufene, Programme; die ausführende Maschine; den Benutzer, der wiederum ein Programm oder auch ein Mensch sein kann) gemacht wurden.

Ebenfalls unklar ist heute die Qualifikation der Entwerfer von IT-Systemen: Jeder darf IT-Systeme entwerfen, produzieren, betreiben, verbinden und modifizieren.

3 Skizze des Spezifischen eines Berufsrechts für Informatiker

Jemand sollte nur dadurch **Informatiker** werden, dass er nach Durchlaufen einer gründlichen fachlichen Ausbildung neben allgemeinen Regeln für Wissenschaftler und Ingenieure folgende informatikspezifische Regeln explizit als verbindlich für seine Arbeit anerkennt:

1. Für jedes (Sub-)System, an dem ein Informatiker mitarbeitet, macht er sich und allen Mitarbeitern sowie durch geeignete Dokumentation den Benutzern klar, um welchen *Systemtyp* (präzis definiert; vage definiert; sozio-technisch, d.h. manche Menschen werden als Teil des IT-Systems betrachtet) es sich handelt, vgl. [Pfit_90]. Damit haben die Schöpfer eines (Sub-)Systems und dessen Benutzer die gleichen Erwartungen an dessen technische Beherrschbarkeit und damit seine maximale Vertrauenswürdigkeit.
2. Ein Informatiker entwirft, produziert, betreibt, verbindet oder modifiziert nur (Sub-)Systeme, nachdem er sich in der dem Systemtyp angemessenen Weise *über alle Schnittstellen informiert und diese vollständig verstanden hat*. Ist ihm dies nicht möglich, so lehnt er die Arbeit am

[35] Da hab ich sprachlich zumindest geschummelt (wenn nicht Schlimmeres): Ich kenne niemand, der gerne kontrolliert wird ... also werden wohl *alle* lieber nicht kontrollierbar arbeiten.

(Sub-)System ab, da zumindest ihm dieses System zu komplex ist, als dass er es im technischen Sinne beherrschen könnte. Findet sich kein Informatiker, der dies kann, so muss das (Sub-)System weiter unterteilt werden oder es müssen einfachere Schnittstellen geschaffen werden.

Die angesprochene Möglichkeit der Arbeitsverweigerung muss durch eine Anpassung des Arbeitsrechts oder eine spezielle Verpflichtung unterstützt werden, durch die Organisationen/Firmen überhaupt erst das Recht zum Entwurf, der Produktion, dem Betrieb, dem Verbinden und Modifizieren von IT-Systemen erhalten, s.u. Andernfalls wäre zu befürchten, dass der Auftraggeber auf – sei es auch qualitativ ungenügender – Erfüllung seines Auftrags besteht und sich ersatzweise zur Übernahme der „persönlichen“ Verantwortung (siehe 4. Regel) bereit erklärt, wodurch in der Praxis wieder der heutige Zustand hergestellt wäre. Leider ist die Abwesenheit von subtilem Druck auf Informatiker, auch für nicht vollständig Verstandenes Erklärungen abzugeben, nur sehr schwer überprüfbar, was das größte Hindernis bei der Einführung des Vorgeschlagenen in der Praxis sein dürfte.

3. Für jedes entworfene, produzierte, betriebene, verbundene oder modifizierte (Sub-)System *S* unterschreibt der Informatiker eine **Erklärung** folgender Art:

   „Wenn *S* die an seinen Schnittstellen zugesicherten Dienste korrekt zur Verfügung stehen, stellt *S* an seinen Schnittstellen die zu erbringenden Dienste korrekt zur Verfügung.“

   Dabei kann durchaus vereinbart werden, dass bei sogenannten fehlertoleranten IT-Systemen beim Auftreten von Fehlern, die die Fehlervorgabe nicht überschreiten [Echt_90], der Umfang der zu erbringenden Dienste – wie spezifiziert – sinkt. Die Erklärung bezeichnet den Systemtyp (präzis definiert, vage definiert, sozio-technisch), der die Präzision des Korrektheitsbegriffs festlegt.

   Das (sinnvollerweise: digitale) Unterschreiben sowie die Zusammensetzung der einzelnen Zusicherungen zu umfassenderen kann (und aus Aufwandsgründen: muss) eine Entwurfsumgebung übernehmen. Vorausgesetzt wird für die Sicherheit der persönlichen digitalen Signaturen natürlich, dass jeder einen (kleinen) Rechner ausschließlich unter seiner persönlichen Kontrolle hat.

4. Jeder Informatiker übernimmt die volle persönliche *Verantwortung* für seine unterschriebenen Erklärungen, an die im Einzelfall auch strafrechtliche und/oder zivilrechtliche Konsequenzen geknüpft werden können. Bei kritischen Systemen etwa sollte man fordern, dass nur Informatiker beteiligt sind, die noch nie eine falsche Erklärung abgegeben haben. Erscheint dies zu rigoros, so kann man verschiedene Sorgfaltsstufen einführen und nur fordern, dass der Informatiker noch nie eine falsche Erklärung in dieser oder einer höheren Sorgfaltsstufe abgegeben hat. Ähnlich kann man im zivilrechtlichen Bereich verfahren und die persönliche finanzielle Haftung (etwa durch eine hinterlegte Summe oder Berufshaftpflichtversicherung) begrenzen, statt sie auf das gesamte Vermögen zu erstrecken. (Insbesondere bei der zivilrechtlichen Haftung kann es bei abhängig beschäftigten Informatikern sinnvoll sein, sie weiterhin dem Arbeitgeber aufzuerlegen.)

   Die Verteilung und – sofern erfolgt – die Begrenzung der Verantwortung ist dem Benutzer des (Sub-)Systems mitzuteilen, so dass er auch hieraus auf den Grad der Vertrauenswürdigkeit schließen kann.

5. Konstruiert ein Informatiker aus Subsystemen ein größeres System, so hat er einerseits die Zusicherungen von Eigenschaften der verwendeten Subsysteme auf Plausibilität und Glaubwürdigkeit zu prüfen: Wer sind die Entwerfer, Produzenten? Was ist ihr informatischer Leumund? Wurden die Subsysteme einer Prüfung durch Dritte unterzogen? Wer hat nach welchen Kriterien geprüft?

   Andererseits sollte er im Zweifelsfall defensiv vorgehen und auf das Subsystem verzichten oder zumindest die zugesicherten Leistungen nicht ausreizen.

6. Um Innovation und Experimentieren weiterhin zu ermöglichen, kann es IT-Systeme geben, die nicht nach obigen Grundsätzen entwickelt wurden. Sie müssen deutlich als solche gekennzeichnet sein und ihr Einsatz sollte die Zustimmung aller Betroffenen voraussetzen.

Um Mißverständnissen vorzubeugen: Insbesondere vage definierte Systemtypen (z.B. Anwendungssysteme, das typische Arbeitsfeld von angewandten, im Gegensatz zu Kerninformatikern) sowie die Erweiterung von (Anforderungs-)Spezifikationen ermöglichen den erwünschten und bereits heute zu beobachtenden pragmatischen Fortschritt im Leistungsspektrum von IT-Systemen weiterhin.

Es sei darauf hingewiesen, dass die geforderte Registrierung, welche Informatiker (noch) in welchen Sorgfaltsstufen beteiligt sein dürfen, nicht unbedingt die Realisierung einer zentralen Überwachungsinstanz bedeutet. Dies kann auch dezentral sichergestellt werden, wozu der „credential“-Mechanismus von David Chaum verwendet werden kann [Chau2_90].

Von der Verbindlichkeit obiger 6 Regeln für *alle* Informatiker verspreche ich mir:

a) Die in der Literatur oft geforderte Spezifikation von überschaubaren (Sub-)Systemen wird tatsächlich praktiziert (Regeln 1-3).
b) Spezifikation und Implementierung werden unverfälschbar dokumentiert (Regel 3). Insbesondere digitales Unterschreiben sichert nicht nur den Benutzer eines (Sub-)Systems vor dem Entwerfer, Produzenten etc., denn der kann den Inhalt der Erklärung nicht bestreiten. Sondern es sichert auch den Entwerfer, Produzenten etc. eines (Sub-)Systems vor dem Benutzer, denn dieser kann nur zugesicherte Dienste fordern und keine für die Diensterbringung notwendigen Voraussetzungen weglassen, indem er sich auf mündliche Absprachen beruft oder die Dokumentation fälscht. Ebenfalls kann der Benutzer beispielsweise nicht Programme verfälschen und behaupten, diese seien ihm geliefert worden und hätten ihm Schaden verursacht.
c) Informatiker werden auf ihren persönlichen „guten Namen“ achten, so dass der Personenbezug der Regeln 3 und 4 zu individuell höherer Sorgfalt anhält, als wenn nur am Schluß die ein Produkt verkaufende Firma eine Erklärung der in Regel 3 beschriebenen Art unterschreiben würde, was für Produkthaftung völlig hinreichend wäre.

   Es sei betont, dass persönlich abgegebene Erklärungen nicht nur erlauben, den „guten Namen“ zu verlieren, sondern auch, ihn zu bewahren: Kein Vorgesetzter und kein Team kann jemandem einfach seine aus seiner Sicht unfertige Arbeit aus der Hand nehmen und zur Benutzung oder gar zum Verkauf freigeben und bei auftretenden Problemen dann doch wieder auf den Urheber verweisen. Außerdem dürfte eine persönliche und unfälschbare Freigabe der eigenen (Sub-)Systeme Arbeitsorganisationsformen mit größerer Autonomie der Arbeitnehmer unterstützen.[36]
d) Durch das Zusammenbinden der Ziele a), b) und c) wird jedes einzelne nachhaltiger erreicht, als wenn es nur einzeln angestrebt würde.

Obigen, auf das Individuum bezogenen Regeln entsprechen solche, denen sich alle Organisationen/Firmen unterwerfen müssen, die IT-Systeme entwerfen, produzieren, betreiben, verbinden oder modifizieren.

Es ist wichtig, sich klarzumachen, dass wenn man Verantwortung Individuen zuordnen *kann*, eine Vergröberung der Zuordnung zu Teams bzw. Organisationen/Firmen *leicht* ist und aus dem Können

---

[36] Dass damit auch unerwünschten Effekten Vorschub geleistet wird, wie Drängen von Informatikern in eine scheinbare Selbständigkeit (etwa als Freier Mitarbeiter oder als Vertragspartner bei Werkverträgen mit faktischer Abhängigkeit von einem Auftraggeber), so dass Krankheit oder allgemeiner Arbeitsunfähigkeit dann allein das Risiko des bisherigen Arbeitnehmers ist, sollte ich explizit erwähnen.

kein *Müssen* folgt. Das Umgekehrte gilt leider nicht: Das Wissen, dass z.B. ein Team einen Fehler gemacht hat, ermöglicht es im allgemeinen nicht festzustellen, wer im Team ihn gemacht hat.

Mein Vorschlag behindert Arbeitsteilung, insbesondere Software-Engineering, also nicht, sondern unterstützt sie sogar. Am Ende der Entwicklung kann automatisch geprüft werden, ob die zu erbringenden Dienste des Gesamtsystems mittels der abgegebenen Erklärungen aus den zugesicherten Diensten (im Grenzfall: den für zutreffend gehaltenen Naturgesetzen) hergeleitet werden können. Bei erfolgreicher Prüfung unterschreibt die prüfende Instanz eine Erklärung für das Gesamtsystem. Bei fehlgeschlagener Prüfung wird klar, wo Verantwortungsdefizite stecken. (Die hier geforderten Erklärungen können technisch wie in [ClPf_91] beschrieben realisiert werden. Zusammen ergibt sich ein umfassendes System zur Übernahme und ggf. späteren Zuweisung von Verantwortung beim Auftreten von „Fehlern“.)

Eine Organisation/Firma erhält das Recht zum Entwurf, der Produktion, dem Betrieb, dem Verbinden oder Modifizieren von IT-Systemen nur dann, wenn

- die Entstehungsgeschichte ihrer (Sub-)Systeme lückenlos durch Erklärungen von Informatikern abgedeckt ist und
- sie keinen Druck auf Informatiker ausübt, für nicht vollständig Verstandenes Erklärungen abzugeben.

Erscheint dies zu rigoros, so können – wie oben bezüglich Individuen beschrieben – verschiedene Sorgfaltsstufen unterschieden werden.

Es bleibt noch festzulegen, welche Institution das Recht zum Entwurf, der Produktion, ... von IT-Systemen verleiht. Die Möglichkeiten reichen von der GI bis zum Wirtschaftsministerium. Da ein erheblicher Teil der IT-Systeme aus dem Ausland importiert wird, stellt sich die Zulassungsfrage auch dort oder spätestens beim Import von Informationstechnik.

4 Was ist von wem zu tun?

Zunächst müssen diese informatikspezifischen Regeln auf Relevanz und vor allem Vollständigkeit geprüft werden. Ggf. sind weitere herauszuarbeiten[37].

Es muss diskutiert werden, ob und ggf. durch welche natur- oder ingenieurwissenschaftliche Kodizes oder gar allgemeinmenschliche Kodizes sie ergänzt werden sollen, vgl. die angeführte Literatur.

Es ist zu entscheiden, was ethischer Kodex werden und was zu Recht gerinnen soll.

Danach ist noch viel Formulierungssorgfalt nötig.

Bezüglich einer Einführung eines ethischen Kodexes bzw. Berufsrechts für Informatiker hoffe ich einerseits auf die Unzufriedenheit der *Benutzer* heutiger IT-Systeme, die oftmals nicht primär dem Menschen Arbeit abnehmen, sondern ihn durch Verschleierung der Verantwortlichkeiten letztlich von aller Verantwortung befreien. Man denke nur an in Verwaltungen häufig gehörte Entschuldigungen: „Das kann unser Computer leider nicht.“ oder „Da muss unser Computer einen Fehler gemacht haben.“

Andererseits hoffe ich auf das Eigeninteresse der Informatiker als Berufsgruppe, es nicht schwarzen Schafen und, wegen der weitreichenden Konsequenzen von Schlampigkeit, Zeitdruck etc., auch nicht grau gesprenkelten zu überlassen, weiterhin das Berufsbild in der interessierten Öffentlichkeit zu prägen.

---

[37] Vielleicht sind auch manche zu modifizieren oder zu streichen ;-).

5 Was bleibt trotz Dokumentation der Verantwortlichkeiten und Berufsrecht offen?

Keine noch so genaue Dokumentation der Verantwortlichkeiten und auch kein Berufsrecht für Informatiker kann verhindern, dass

- unerkannte „Fehler“ dauerhafte Auswirkungen haben, etwa vertrauliche Information von einem Trojanischen Pferd über einen verdeckten Kanal zu einem interessierten Empfänger übertragen wird, und dass
- auch der erste erkannte Fehler nicht wiedergutzumachende Auswirkungen haben kann, etwa das Versagen einer Kernkraftwerkssteuerung.

Hier helfen nur vorbeugende Schutzmaßnahmen, z.B. wo möglich bereits das Vermeiden der Erfassungsmöglichkeit von Daten und die Begrenzung des Schadenspotentials von Anwendungen, ggf. also auch der Verzicht auf solche mit zu hohem Schadenspotential.

Eine bessere Kontrolle der entworfenen IT-Systeme ist der hier als Notmaßnahme vorgeschlagenen Kontrolle ihrer Entwerfer und der bereits weitgehend praktizierten Kontrolle ihrer Benutzer (etwa durch intensive Protokollierung ihres Tuns) also vorzuziehen. Hierfür wird rechnergestützte Verifikation zukünftig hoffentlich einen wesentlichen Beitrag leisten können. Dort, wo sie erfolgreich angewendet werden kann, kann und sollte die Kontrolle der Entwerfer von IT-Systemen entsprechend reduziert werden.

Ein Dankeschön

Für Kritik und Anregungen danke ich Gerrit Bleumer, Manfred Böttger, Dirk Fox, Birgit Pfitzmann, Prof. Dr. Reinhard Voßbein, Dr. Michael Waidner und zahlreichen Diskutanten im GRVI / GDD / DVD / DGIR / GI-Diskursprojekt „Rechtliche Beherrschung der Informationstechnik“ herzlich.

Zitierte Literatur

Chau2_90 David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Intern. Conf. on Cryptology, Sydney, Australia, January 1990, AUSCRYPT '90, LNCS 453, Springer-Verlag, Berlin 1990, 246-264.

ClPf_91 Wolfgang Clesle, Andreas Pfitzmann: Rechnerkonzept mit digital signierten Schnittstellenprotokollen erlaubt individuelle Verantwortungszuweisung; Datenschutz-Berater 15/8-9 (1991) 8-38.

Echt_90 Klaus Echtle: Fehlertoleranzverfahren; Studienreihe Informatik, Springer-Verlag, Heidelberg 1990.

Pfit_90 Andreas Pfitzmann: Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung; Datenschutz und Datensicherung DuD 14/12 (1990) 620-627.

Literatur zu Ethische Kodizes für Wissenschaftler und Ingenieure

Association for Computing Machinery: Bylaw 21. ACM Code of Professional Conduct; Communications of the ACM 23/7 (1980) 425.

Ronald E. Anderson, Deborah G. Johnson, Donald Gotterbarn, Judith Perrolle: Using the ACM Code of Ethics in Decision Making; Communications of the ACM 36/2 (1993) 98-107 {enthält auch den Text des „ACM Code of Ethics and Professional Conduct“ vom Okt. 1992}.

Edward C. Bertnolli, Robert Alden, William Middleton, William Tackaberry, Steven Unger: Proposed new Code of Ethics released by ad hoc committee; The Institute, IEEE, 14/3 (1990) 5.

The British Computer Society: Code of Practice; 13 Mansfield Street, London W1M 0BP.

The British Computer Society: Code of Conduct; 13 Mansfield Street, London W1M 0BP.

C. Dianne Martin, David H. Martin: Professional Codes of Conduct and Computer Ethics Education; Computers & Society 20/2 (1990) 18-29.

William W. Middleton: Does the IEEE Code of Ethics need fixing? IEEE-USA unit's proposed Code; The Institute, IEEE, 14/7 (1990).

Edward A. Torrero: Board backs new code; IEEE Code of Ethics; The Institute, IEEE, 14/9 (1990) 2.

Panel to eye response to plan for changes in Ethics Code; The Institute, IEEE, 13/4 (1989) 11.

Emerson W. Pugh: Must we give up ethics to eat?; The Institute, IEEE, 13/4 (1989) 6.

Hal Sackman: Preliminary IFIP Code of Ethics; IFIP Newsletter December 1989.

Verein Deutscher Ingenieure (VDI): Bekenntnis des Ingenieurs; Düsseldorf, den 12. Mai 1950.

Joel Rothstein Wolfson: A Code of Professional Responsibility -- An Ethics Code With Bite; Proc. of the Conf. on Computers and the Quality of Life (CQL '90), Sept. 13-16, 1990, Washington, computers & society, SIGCAS, ACM, 20/3 (1990) 192.

Literatur zu Verantwortung von Wissenschaftlern und Ingenieuren

Donald Christiansen: Ethical dilemmas revisited; IEEE spectrum 26/4 (1989) 21.

Literatur zu Verantwortung von Informatikern

Joachim Biskup: Verantwortung des Hochschullehrers für Informatik; Informatik-Spektrum 12/3 (1989) 158-161.

Committee on Public Policy: Draft 7B: Entity Position Paper on Software Vandalism; Computer, IEEE, 22/7 (1989) 83-84.

Wolfgang Coy: Brauchen wir eine Theorie der Informatik?; Informatik-Spektrum 12/5 (1989) 256-266.

Michael C. McFarland: Urgency of ethical standards intensifies in computer community; Computer, IEEE, 23/3 (1990) 77-81.

Susan J. Harrington, Rebecca L. McCollum: Lessons from Corporate America applied to Training in Computer Ethics; ACM SIGSAC Review 8/3 (1990) 23-28.

Harold Joseph Highland: Random Bits & Bytes; Computers & Security 7/5 (1988) 439-449.

Hans Lenk: Können Informationssysteme moralisch verantwortlich sein?; Informatik-Spektrum 12/5 (1989) 248-255.

Nilakantan Nagarajan: What's Computer Ethics, anyway?; SIGSAC Review, acm, 8/2 (1990) 24-32.

Helen Nissenbaum: Computing and Accountability; CACM 37/1 (1994) 73-80.

Richard Parker: Computer-related crime: Ethical considerations (with applications for teaching computer literacy classes); ACM SIGSAC Review 8/3 (1990) 13-22.

Ralph J. Preiss: Action needed on computer ethics legislation; Computer, IEEE, 23/2 (1990) 74.

Karl-Heinz Rödiger, Wolfgang Coy, Günther Feuerstein, Rolf Günther, Werner Langenheder, Bernd Mahr, Peter Molzberger, Hartmut Przybylski, Horst Röpke, Eva Senghaas-Knobloch, Birgit Volmerg, Walter Volpert, Hellmut Weber, Herbert Wiedemann: Informatik und Verantwortung; Arbeitskreis 8.3.3 "Grenzen eines verantwortbaren Einsatzes von Informationstechnik" der Gesellschaft für Informatik; Informatik-Spektrum 12/5 (1989) 281-289.

Eric A. Weiss: The XXII Self-Assessment: The Ethics of Computing; Communications of the ACM 33/11 (1990) 110-132.

Jan Witt: Dogma und Skepsis; Gedanken zur Angemessenheit der aktuellen Technik-Kritik im Bereich der Informatik; Informatik-Spektrum 12/5 (1989) 274-280.

Artikelsammlungen

Artikel von Reinhard Stransfeld, Peter Schefe, Sybille Krämer, Bernd Mahr und Bernd Lutterbeck in Wolfgang Coy et al. (Hrsg.): Sichtweisen der Informatik, Vieweg, 1992.

D. G. Johnson, J. W. Snapper: Ethical Issues in the Use of Computers; Belmont, Wadsworth 1985.

IFIP-WG9.2 On Behalf of IFIP-TC9: Ethics of Computing: Information Technology and Responsibility; To Promote Discussion Inside the IFIP National Societies; Madrid, september 1992.

Sitzung „Ethics of Computing: Information Technology and Responsibility“, Education and Society; Information Processing 92; IFIP Transactions A-13, North-Holland, 344-373.

Lesetipps

Vermittlung und Umsetzung Ethischer Leitlinien

In IEEE spectrum 35/6 (June 1998) Seite 51-61 finden Sie einen lesenswerten Artikel darüber, wie Ethische Leitlinien vermittelt und ihn Organisationen umgesetzt werden können.

Ein Leitfaden zur verantwortungsvollen Nutzung von Datennetzen

siehe URL `http://www.hrz.uni-dortmund.de/docs/Netzleitfaden.html`

Eine Reflexion über Wirtschaftsinformatik und Ethik

Georg Fehling, Bernd Jahnke: Wirtschaftsinformatik und Ethik – Komplementarität oder Konkurrenz? Informatik-Spektrum 22/3 (1999) 197-205

Ethik als empirische Wissenschaft

Hermann Rampacher: Ethik als exakte empirische Wissenschaft; Mit Anwendungsbeispielen aus der Informatik; FiFF-Kommunikation 20/4 (Dezember 2003) 9-13

Benimmregeln für Roboter ?

Zu 1/4 Ernst, zu 3/4 Spaß – oder war es doch 1/*e* gegenüber 1 - 1/*e* – nachfolgend eine Zusammenfassung von Roger Clarke: Asimov's Laws of Robotics: Implications for Information Technology; Computer (Dez. 1993) 53-61 und (Jan. 1994) 57-66.

Isaac Asimov, 1920-1992, Chemiker, Biochemiker und später Science-Fiction-Schreiber;

Ziel: Entwurf einer Menge von Regeln, die verlässliche Kontrolle halbautonomer Maschinen erlauben.

„A robot is ‚a reprogrammable multifunctional device designed to manipulate and/or transport material through variable programmed motions for the performance of a variety of tasks.' The term robotics – which Asimov claims he coined in 1942 – refers to ‚a science or art involving both artificial intelligence (to reason) and mechanical engineering (to perform physical acts suggested by reason).'“

Neben offensichtlichen möglichen Vorteilen für Menschen könnten Roboter Menschen oder ihr Eigentum direkt oder indirekt verletzen. Zusätzlich kann das Ersetzen von Menschen durch Maschinen die Selbstachtung der Betroffenen untergraben und vielleicht sogar die der Menschen allgemein.

Asimov's Laws of Robotics (1940)

First Law:
A robot may not injure a human being, or, through inaction, allow a human being to come to harm.

Second Law:
A robot must obey the orders given it by human beings, except where such orders would conflict with the First Law.

Third Law:
A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Da die Gesetze in die Maschine hineinentworfen werden, sollte es ihr niemals in den Sinn kommen, sie zu brechen.

Um die Gesetze befolgen zu können, müssen Roboter Menschen und Roboter unterscheiden können, ebenso Befehle (order) von Wünschen (request).

Widersprüchliche Befehle müssen priorisiert werden, etwa wenn zwei Menschen Widersprüchliches anordnen.

Unsinnige oder ungesetzliche Befehle müssen als solche erkannt und ggf. nicht ausgeführt oder zumindest in Frage gestellt werden.

Das erste Gesetz ist nicht absolut: Was, wenn das Verletzen eines Menschen die Leben zweier anderer rettet, dreier oder gar einer Million Menschen?[38]

Nach diesen Gesetzen agierende Roboter sind ungeeignet, Kinder oder Gefangene zu beaufsichtigen.

---

[38] Im Film „I, Robot“ von 2004 (sehenswert!) führt diese Überlegung dazu, daß die Roboter versuchen, die Kontrolle über die Menschen zu übernehmen, um so Verletzungen von Menschen langfristig zu minimieren. Die Roboter geben also dem First Law in ihrer neuen, umfassenderen Interpretation ganz klar Priorität vor dem Second Law.

1950 entdeckte Asimov eine Notwendigkeit, das erste Gesetz auszuweiten, Zeroth Law, s.u.

Dadurch werden Roboter zunehmend gezwungen, mit Abstraktionen und philosophischen Dingen klarzukommen.

Mit dieser zusätzlichen Regel erscheint es wahrscheinlicher, dass Roboter eine dem Menschen übergeordnete, väterliche Rolle einnehmen.

Asimov's revised Laws of Robotics (1985)

Zeroth Law:
A robot may not injure humanity, or, through inaction, allow humanity to come to harm.

First Law:
A robot may not injure a human being, or, through inaction, allow a human being to come to harm, unless this would violate the Zeroth Law of Robotics.

Second Law:
A robot must obey orders given it by human beings, except where such orders would conflict with the Zeroth or First Law.

Third Law:
A robot must protect its own existence as long as such protection does not conflict with the Zeroth, First, or Second Law.

Aus Sicht von Roger Clarke müssen einige, in den Geschichten von Asimov nur implizit enthaltene Gesetze ergänzt werden (es gilt jeweils: Law *n* a) ist higher order than Law *n* b)):

An extended set of the Laws of Robotics (Roger Clarke, 1994)

The Meta-Law:
A robot may not act unless its actions are subject to the Laws of Robotics.

Law Zero:
A robot may not injure humanity, or, through inaction, allow humanity to come to harm.

Law One:
A robot may not injure a human being, or, through inaction, allow a human being to come to harm, unless this would violate a higher order law.

Law Two:
a) A robot must obey orders given it by human beings, except where such orders would conflict with a higher order law.
b) A robot must obey orders given it by superordinate robots, except where such orders would conflict with a higher order law.

Law Three:
a) A robot must protect the existence of a superordinate robot as long as such protection does not conflict with a higher order law.
b) A robot must protect its own existence as long as such protection does not conflict with a higher order law.

Law Four:
A robot must perform the duties for which it has been programmed, except where that would conflict with a higher order law.

The Procreation Law:
A robot may not take any part in the design, manufacture, or maintenance of a robot unless the new or modified robot's actions are subject to the Laws of Robotics.

Alle Gesetze spiegeln humanitäre und egalitäre Prinzipien wider. Dies im Gegensatz zum üblichen Umgang mit Informationstechnologie, wo der Besitzer eines Gerätes implizit als der durch es primär Begünstigte angenommen wird.

Nachfolgend noch etwas aktuelles Material:

Im ZEIT-Magazin...

Auf folgende Tagungsankündigung gab es folgenden offenen Brief:

Date: Tue, 19 Mar 1996 20:17:20 PST
From: ben@cs.umd.edu (Ben Shneiderman)
Subject: response to a conference posting
To: announcements.chi@xerox.com

On February 13, 1996 a disturbing notice about a conference on Autonomous Agents was posted to this SIGCHI list (announcements.chi@xerox.com). I have taken more than a month to consider responding, but I feel that I must if I am to adhere to the ACM's Code of Ethics (CACM Feb 1993, 98-107), which calls on "computing professionals to minimize negative consequences of computing systems (Section 1.1)." The principle of "Avoid harm to others" (Section 1.2) is accompanied by the clear statement that "the individual computing professional is responsible for any resulting injury." I consider the conference on Autonomous Agents to be leading towards a reduced sense of programmer and user responsibility for negative outcomes of computer applications.

The conference announcement indicates (emphasis added):

This conference will bring together researchers interested in modeling and building autonomous agents. Agents are computational systems that INHABIT dynamic, unpredictable environments. THEY INTERPRET sensor data that reflect events in the environment and EXECUTE MOTOR COMMANDS that produce effects in the environment. An agent is "autonomous" to the degree that IT DECIDES FOR ITSELF how to relate sensor data to motor commands IN ITS EFFORTS TO ACHIEVE GOALS, SATISFY MOTIVATIONS, etc.

I believe that the suggestion that these agents inhabit, interpret, decide, or satisfy motivations is misleading. The repeated use of "autonomous" with the implication that no human is responsible for the results violates the ACM Code of Ethics. If programmers reject responsibility for their programs, they may be less diligent in avoiding information destruction, privacy violation, and physical harm.

I hope the organizers of the Conference on Autonomous Agents will change the statement of goals and title to recognize human responsibility for the actions of any program. Their emphasis on autonomy and the anthropomorphic language are misleading to designers, researchers, and the public. Since language shapes action, a more appropriate, but less exciting, title (or subtitle) might be: Designing Levels of Supervisory Control for Planned Procedures. Tom Sheridan's work on supervisory control (for example in nuclear reactor control rooms) constructively addresses the dangers and benefits of automaticity.

Furthermore, it is ironic that the organizers would post their notice to the SIGCHI list and not even include user interface design or human-computer interaction among their list of topics. Even basic

issues such as programming or specification of planned procedures (agents) is avoided, thereby contributing to the impression that these planned procedures (agents) have a life of their own and appear magically without human action.

I am encouraged by and recommend reading Fred Brooks' thoughtful article "The Computer as Toolsmith" (CACM March 1996, 61-68). He celebrates the movement from early efforts to make machines that think to more recent projects for giving users better control over computers.

The key issue is responsibility. The conference organizers might make more significant research contributions if they recognized multiple levels of operator control and responsibility in tele-operation, networked, and rapid real-time situations.

Copies to conference organizers: johnson@isi.usc.edu (Lewis Johnson) bhr@hpp.stanford.edu (Barbara Hayes-Roth) maes@media.mit.edu (Pattie Maes) wex@media.mit.edu (Alan Wexelblat, sender of announcement)

Sincerely,
Ben Shneiderman email: ben@cs.umd.edu
Dept. of Computer Science (301) 405-2680
University of Maryland (301) 405-6707 FAX
College Park, MD 20742 `http://www.cs.umd.edu/projects/hcil`

X-Sender: schefe@rzdspc1.informatik.uni-hamburg.de (Unverified)
Mime-Version: 1.0
Date: Mon, 1 Apr 1996 12:21:26 +0100
To: fiff-l@dia.informatik.uni-stuttgart.de
From: schefe@informatik.uni-hamburg.de (Peter Schefe)
Subject: Ben Shneiderman's response to...

Peter Schefe: Some Comments on B. Shneiderman's Response to the Announcement of a "Conference on Autonomous Agents"

"The key issue is responibility". I agree with J. Friedrich that this is the central proposition of B. Shneiderman's reaction to a conference posting concerning "autonomous agents". I would like, however, to have a closer look to what are the the non-obvious presuppositions and implications of Shneiderman's statement. What kind of responsibility does he mean? This question falls into several subquestions.

First, which role was Shneiderman taking on when feeling that he must react to the posting? If he refers explicitly to the ACM Code of Ethics, the obvious answer is: as a computer professional, especially an ACM member. But why did he hesitate to react? Why wasn't he sure about that? Was there a conflict of roles? Although he fails to give any hint, I would suggest the following: he should have known about "autonomous agents" before. This seems quite probable, as all relevant aspects of agents addressed by Shneiderman have been published earlier, for example in the July 1994 issue of CACM. He didn't respond to that as far as I know. Why? The posting elicitating his

reaction was published in SIGCHI. This seems to indicate another role given by his outstanding involvement with and expertise in this field: Shneiderman reacts as an CHI expert.

Second, to whom does Shneiderman feel responsible? As an individual, he feels responsible to his profession, especially, in accordance with the observations above, to the community of his CHI peers. This may resolve an institutional conflict. The conference initiators are members of the professional community representive of an even greater part thereof. Thus, there may be a conflict of adhering to the institutional Code and to be loyal to a considerable subcommunity of the profession.

Third, according to which type of ethics does Sheiderman engage himself? In the first place, he mentions the adherence to the Code. He views himself as acting conformable to his duty. The ACM Code strongly supports an deontological ethics. The individual is obliged to behave according to certain commandments. Always be honest and trustworthy! Individualistic codes of ethics have its merits in supporting individuals in situations of conflict. If I am right, Shneiderman is in such a situation. However, I think he is also a consequentialist hoping that his action will contribute to a change that will „minimize negative consequences". Will it? Even assuming that his assessment is correct, it can be doubted that his individual intervention will have the desired consequences. Only the
exertion of institutional power (sanctions or gratifications) could be expected to change the behaviour of people. Shneiderman refers to an institution (the Code) without much power (termination of ACM membership does not make sense here). Whether Shneiderman's assessment is correct, can be doubted as well.

This is corroborated by answering the questions: What is his concern? For whom does he feel responsible? Once more, the key is responsibility. Talking of "autonomous agents", Shneiderman conjectures, is "misleading", having the implication "that no human is responsible", and having as a consequence "a reduced sense of programmer and user responsibility". Programmers and users are the people he is solicitous about. Is his concern justified? Do his concerns justify his intervention?

I think it is true that metaphors can influence design, even express or give rise to research programmes (which is probably true in the case of agent technology in general). However, his argument that programmers be less diligent if programming agents is quite unconvincing. As to the users, it is up to them to decide upon the degree of "autonomy" of their agents (P. Maes). Hence, contrary to Shneiderman's apprehension, to unleash agents may enhance the user's sense of responsibility. Nevertheless, I would agree that "autonomy" is a possibly misleading metaphor, if it is not made clear that the implication is not an autonomy of action, but simply a programmed adaptivity of machine behaviour. The "goals" of "agents" are not intended by a machine, but are intentional interpretations of their designers and users. Algorithmic machines can be viewed as abstracted decision procedures pertaining to formal subgoaling, choice of means etc. However, they are blind to intentions purposes, and values.

Shneiderman appears to be opposed to "anthropomorphic language" in general. I think computer science cannot do without some anthropomorphic metaphors (even "control" and "data" are anthropomorphic metaphors). I have no problem with "interpretation of sensor data", for instance. Admittedly, "motivation" may raise one's eyebrows, but it can be given a restricted interpretation in the sense mentioned above. On the other hand, the "toolsmith" metaphor is misleading if applied to "autonomous" information seeking or filtering mechanisms, not to mention to world-wide computer networks. "Controlling" these is not adequately addressed by the tool metaphor. Problems that have

shown up so far, are not due to "language" but to actual use of these devices in a complex socio-computational environment. Beyond that - our artifacts have long acquired "autonomy". To call them "tools" is at least as misleading to the public as to call them "autonomous agents". Providing with more "levels of operator control" may be a useful rationale for constructing interfaces, however, it does not address the problem of shaping complex socio-technical systems.

Prof Dr. Peter Schefe
Universitaet Hamburg
Fachbereich Informatik/ASI
Vogt-Koelln-Str. 30 Tel.: 040/54715-427 -425 (Sekr.)
22527 Hamburg Fax-Nr.: 040/54715-303

Aufgabe

Diskutieren Sie (vorzugsweise in einer kleinen Gruppe), ob es realistisch ist zu erreichen, dass sich *alle* Roboter (d.h. *alle* halbautonomen Maschinen) an eine Menge von Regeln halten werden?
Wenn Sie meinen ja, dann lesen Sie mal

> „Die Demokratisierung des Bösen – Ist der Mensch reif für die Möglichkeiten, die der technische Fortschritt bietet?“ Ein ZEIT-Interview zwischen Christian Tenbrock und dem Computerforscher Bill Joy `http://www.zeit.de/archiv/2000/13/200013.bill-joy-intervi.xml`.

Danach kann es sich lohnen, die Diskussion fortzusetzen.

Open Source: Motive, Vorgehen und bisher Erreichtes

Open Source ist aus meiner Sicht das Informatik-Schlagwort des Jahres 1999. Dies hat eine lange Vorgeschichte, die über Softwareprojekte (GNU, Linux, etc.) weit ins Gesellschaftsphilosophische, ja geradezu Gesellschaftskommunitäre geht.

Literatur:

`http://www.opensource.org/`

Fiff-Kommunikation 3/99

Ludwig Siegele: Lieber Ruhm im Netz als Rubel im Sack; DIE ZEIT Nr. 12, 16. März 2000, Seite 38

`http://www.archiv.zeit.de/daten/pages/200012.open_content_.html`

Open Content `http://www.opencontent.org/`

Tim O'Reilly: Schlüsse aus der Open-Source-Software-Entwicklung

`http://www.heise.de/tp/deutsch/special/wos/6433/1.html`

Informatik und Behinderte

Neben einer sehr guten Seminarausarbeitung

Mareike Freund: Informatik und Behinderte; Univ. Hildesheim 1993,

die bei mir jederzeit kopiert werden kann, sind

Joseph J. Lazzaro: Windows 95: Aiding the Disabled; Byte October 1996, 59-60

Joseph J. Lazzaro: Helping the Web help the disabled; IEEE spectrum 36/3 (1999) 54-59

Fiff-Kommunikation 17/2 (Juni 2000), Themenheft „Informationstechnik und Behinderung“

Leseempfehlungen. Alle behandeln, welche Ein- und Ausgabehilfen Körper-, Seh- und Hörbehinderten den Umgang mit Rechnern erleichtern oder gar erst ermöglichen.

Geschlechtsspezifischer Umgang mit Informationstechnik ?

Gerade zu diesem Themenbereich dürfte jede(r) viele sehr persönliche Erfahrungen und (Vor)Urteile haben. Vielleicht lohnt es sich, sie mit den folgenden 2 Statistiken zu konfrontieren:

Die Deutschen und die Technik (DIE ZEIT Nr. 16 (11. April 1997) Seite 35)
"Nach einer im Auftrag des Verbandes Deutscher Elektrotechniker durchgeführten Studie bejahen vier von 5 Bundesbürgern die Entwicklung neuer Techniken. Favorit ist die Medizintechnik, in der 78 % der Frauen und 71 % der Männer stärkeres Engagement befürworten. Diskrepanzen zeigten sich bei der Energietechnik (Frauen: 47 % Zustimmung, Männer: 65 %), bei der Elektronik (33 und 57) und bei der Informationstechnik (30 und 50). Mit 16 Prozentpunkten bei den Frauen und 22 bei den Männern schnitt die Gentechnik ab, und ganz schlecht mit 8 und 21 Prozent die Kerntechnik."

Etwas übersichtlicher dargestellt:

Für Entwicklung neuer Technik im Bereich ... sind ... in %	**Frauen**	**Männer**
Medizintechnik	78	71
Energietechnik	47	65
Elektronik	33	57
Informationstechnik	30	50
Gentechnik	16	22
Kerntechnik	8	21

Akademikerinnen in der Berufswelt (DIE ZEIT Nr. 22 (23. Mai 1997) Seite 16)
"Nie waren sie so gebildet wie heute: Über ein Drittel aller Berufstätigen mit Studienabschluß sind in der Bundesrepublik Frauen. Allerdings haben die Akademikerinnen ausgesprochen traditionelle Vorlieben: Sie arbeiten häufiger als Männer im Bildungs- und Erziehungssektor, äußerst selten sind sie hingegen in ingenieurwissenschaftlichen oder mathematischen Berufen zu finden. In einem Punkt allerdings gleichen sich die meisten Branchen: Spitzenplätze werden hierzulande trotz aller Bildung immer noch selten mit Frauen besetzt. In der gesamten deutschen Wirtschaft beispielsweise sind gerade einmal sechs Prozent der Führungskräfte weiblich – ein äußerst bescheidenes Ergebnis."

Anteil der Frauen an allen Erwerbstätigen mit Hochschul- oder Fachhochschulabschluß ... in %	**1985**	**1995**
Erziehung, Bildung, Theologie	51	58
Sprach- und Kulturwissenschaften	52,5	55
Medizin, Sozialwesen	38	48
Alle Berufe	*28*	*34*
Agrar-, Forst- und Ernährungswissenschaften	27	33
Rechts- und Verwaltungswissenschaften	18	29,5
Wirtschaftswissenschaften	13	27,5
Mathematik	15	22,5
Ingenieurwissenschaften	4,5	11

Quelle: Stat. Bundesamt, iw, (entnommen DIE ZEIT Nr. 22 (23. Mai 1997) Seite 16))

Punktabzug für Frauen (DIE ZEIT Nr. 22 (23. Mai 1997) Seite 31)

Wissenschaft: Das Wort allein heischt Ehrfurcht vor der Objektivität. Doch ausgerechnet eine nach allen Regeln der Wissenschaft erarbeitete Studie wirft nun einen Schatten auf die Lichtgestalt.

Christine Wenners und Agnes Wold von der Universität Göteborg haben einen statistisch geschärften Blick auf das Innerste der Wissenschaft geworfen: auf die *peer review*. Der Begriff bezeichnet das wissenschaftsübliche Verfahren, in dem anonyme Gutachter ihr Votum darüber abgeben, ob eine Arbeit veröffentlicht werden oder ein Forscher Geld bekommen soll.

Die beiden Schwedinnen erhielten Zugang zu den Akten sämtlicher *peer reviews*, die im Jahre 1995 über die Aufnahme von Post-Docs in den medizinischen Forschungsrat des Landes mitentschieden haben. Das Ergebnis ist die erste empirische Studie über *peer reviews*, der interne Originaldaten zugrunde lagen. Und es ist erschreckend: Frauen wurden durch die Bank schlechter bewertet als Männer mit gleicher wissenschaftlicher Produktivität (diese wiederum wurde für die Studie nach sechs meßbaren Kriterien beurteilt). Außerdem wurden die Antragssteller, die berufliche Verbindungen zu den Gutachtern hatten, signifikant besser beurteilt.

Die Studie erschien in der Zeitschrift *nature* (Bd.387, Nr. 6631, S. 327 ff.). Das Blatt ist *peer reviewed*.

Was tun Frauen in der Informatik (Computer Zeitung Nr. 38 / 18. September 1997, Seite 24)
Neben vielen Beispielen und der Kurzantwort „Alles“ auf die Frage, enthält diese von der GI geschaltete Anzeige folgende Zahlen:

	Frauenanteil gesamt	Frauenanteil bei Neueinschreibungen
Wintersemester 1987/88	13 %	15 %
Wintersemester 1995/96	7,5 %	9,15 %

Frauenanteil am Informatik-Studium

Als Erklärung wird angeboten: „Nicht zu unterschätzen ist der Einfluß, den das Schulsystem auf die Wahl des Berufsweges hat. Unabhängig voneinander berichten viele Lehrerinnen und Lehrer, dass der Informatikunterricht in gemischten Schulen sehr von Jungen dominiert wird. Mädchen verfügen generell über weniger PC-Vorerfahrung und lassen sich durch die Dominanz ihrer Mitschüler oft einschüchtern. Christine Roloff, Sigrid Metz-Göckel u.a. haben 1987 in einer wissenschaftlichen Untersuchung belegt, dass 41 % aller Studentinnen in Mathematik, Naturwissenschaften und Technik aus den 3,8 % reinen Mädchenschulen des Landes Nordrhein-Westfalen stammen.“

Literaturliste von Prof.Dr. Margrit Falck / FHVR Berlin: (Stand: 5.7.1994) zum Thema: Computer und Frauen

K. Behnke, P. Günzler, Anja Hentschel, U. Lindner-Kostka, B. Paech: Was tut die Gesellschaft für Informatik für die Informatikerinnen? Eine Untersuchung zur Arbeitswelt von Frauen in der EDV; Informatik-Spektrum (1994) 17:179-183

W. Coy, F. Nake, J.-M. Pflüger, A. Rolf, J. Seetzen, D. Siefkes, R. Stransfeld (Hrsg.): Sichtweisen der Informatik. Wiesbaden: Vieweg 1992

Tom DeMarco, Thimothy Lister: Wien wartet auf Dich - Der Faktor Mensch im DV-Management. - Hanser: München 1991

M. Falck, S. Gensior, M. Manacorda, U. Meier, G. Paetzold, I. Wagner, R. Wenzlaff: Womans Computers and Participation. — In: P. Docherty, K. Fuchs-Kittowski, P. Kolm, L. Mathiassen (ed.): System Design for Human Development and Productivity: Participation and beyond. Proc. of IFIP TC 9/WG 9.1, 12.-15.5.1986, Berlin, GDR. Elsevier Publ. Amsterdam 1987, S. 457

U. Hoffman: Computerfrauen. München: Rainer Hampp Verlag 1987, S. 78

Susanne Maaß: Informatik - Studium ohne akzeptables Berufsbild. - In: Arbeitspapier zur Tagung "Erfahrung und Abstraktion - Frauensichten auf die Informatik", Mitteilungen des Fachbereichs Informatik der Universität Hamburg, FBI-HH-M- 233/93, S. 37ff. (1993)

R. S. Pressman, S. R. Herron: Software-Schock - Risiko und Chance; Hanser: München 1993

Christine Roloff: Hochqualifizierte Frauen in Naturwissenschaft und Technik. Ursachen ihrer Marginalität und Strategien zur Veränderung. — In: WSI Mitteilungen 4/1993, S. 220-229

B. Schinzel: Frauen in Informatik, Mathematik und Technik; Informatik-Spektrum 14 (1991) 1-14

Joy Teague, Valerie Clarke: Fiction and Fact: Students’ and Professionals’ Perception of Woman in Computer Science; Inger V. Eriksson, Barbara A. Kitchenham, Kea G. Tijdens (ed.): Women, Work and Computerization: understanding and overcoming bias in work and education. Proc. of the IFIP TC9/WG 9.1, Helsinki, Finnland 30.06. - 02.07.1991. Elsevier Publ. Amsterdam 1991, S. 347

Friedrich Weltz, Rolf G. Ortmann: Das Softwareprojekt - Projektmanagement in der Praxis; Campus: Frankfurt, New York 1992

Verhaltensweisen in virtuellen Welten

Materialsammlung und ein paar Anmerkungen zum Film: Der Rasenmähermann

Virtual Reality (VR)

Data Glove bis Ganzkörperkondom und Stereo-Bewegtbilder als neue E/A-Möglichkeit zwischen Mensch und Rechner – aber selbst im Film "Rasenmähermann" fehlt noch viel, z.B. Gerüche und Geschmack

gab es VR nicht immer schon beim Lesen von Büchern – Phantasie

Ultraschall-Untersuchungen beim Arzt – wie virtuell ist die dargestellte Realität

Künstliche Intelligenz (KI)

als Gebärneid (insbesondere) der (homosexuellen) Männer (z.B. Alan Turing[39])

VR und KI

Traum vom ewigen Leben[40]

Unterschied zwischen *das Gleiche* und *Dasselbe*

Ersteres bedeutet, bzgl. der relevanten Eigenschaften identisch, letzteres bedeutet identisch – und deshalb bzgl. aller Eigenschaften gleich.

Informatik hat Äquivalenzbegriff, der allein an den äußeren Schnittstellen von Systemen[41] orientiert ist: Zwei Systeme sind gleich, wenn sie sich nach außen gleich verhalten. Wenn sonst keine Eigenschaften beobachtet werden können oder auch nur beobachtet werden, dann neigt mensch dazu, die gleichen Systeme für dieselben Systeme zu halten.

Meiner Meinung ist die Unterscheidung zwischen *das Gleiche* und *Dasselbe* für Menschen aber wesentlich.

Zwei Beispiele:

1. Wenn ich mir von FreundInnen Bücher ausleihe frage ich oft, ob ich, wenn sie mich wirklich bewegen, hineinmalen darf (mein üblicher Stil intensiv zu lesen), wenn ich danach der VerleiherIn ein neues Buch kaufe und zurückgebe. Oftmals bekomme ich als Antwort „Ja“, hin und wieder aber auch „Nein“, nämlich dann, wenn sich für die VerleiherIn mit diesem Buch ganz konkrete Erlebnisse verbinden, die nicht nur an das Buch als Information (da wäre ein neu gekauftes eher besser), sondern auch als materiellen Gegenstand geknüpft sind. Ich verstehe und respektiere das. Das informatisch naheliegende Vorgehen, mir die Frage zu sparen und ggf. das neue Buch so materiell altern zu lassen, dass es nicht mehr vom geliehenen zu unterscheiden ist, kommt mir vollkommen falsch vor.

---

[39] vgl. das ausgezeichnete Buch [Hoch_87]: Rolf Hochhuth: Alan Turing – Erzählung; Rowohlt, Reinbek 1987 (ISBN 3 498 02879 0), insbesondere Seite 38, 58ff, 80f, 146

[40] [Hoch_87 Seite 5]: „Der Naturwissenschaftler, dessen Name mit einem Effekt oder einem Prinzip verbunden ist, kann für alle Zeiten als *unsterblich* gelten.“

[41] Systeme sind aus Subsystemen zusammengesetzt und können selbst wieder Subsystem eines größeren Systems sein.

2. Falls Sie mit Büchern solche Erfahrungen nicht gemacht haben, dann können Sie sich vielleicht vorstellen, wie Sie sich beim Verleihen eines Fahrrades fühlen, mit dem Sie durch halb Europa gefahren sind, wenn Ihnen ein entsprechendes Angebot gemacht wird.

Zumindest diese Unterscheidung geht bei VR und KI verloren.[42]

Was nebenbei so auffiel:

keine berufstätige oder sonstwie relevant nachdenkende Frau (Was bedeutet das für die Weltsicht der den Film Gestaltenden?)

üble religiöse Klischees, üble religiöse Ausdrucksmittel (Kreuzigung im virtuellen Raum)

Parapsychologie

Mein persönliches Resümée:

Die Gefahr ist nicht, dass die Rechner so werden wie die Menschen, sondern die Menschen so werden, wie die Rechner. Seien Sie – im Ihretwillen – da etwas auf der Hut.

Zitate aus: Marie-Anne Berr: Technik und Körper; (Historische Anthropologie 11) Dietrich Reimer Verlag, Berlin 1990, zugleich Diss. Berlin, Freie Universität.

Seite 135

Denn "das Verhalten der stochastischen Maschine liefert ... eine erstaunlich exakte Beschreibung durchschnittlichen menschlichen Verhaltens. ... Die Maschinentypen, auch die stochastischen Maschinen, scheinen zwar – auf das menschliche Verhalten bezogen – eine Reduktion von Vielfalt darzustellen. Doch muss man davon ausgehen, dass auch dem menschlichen Verhalten durch Normen, Regeln und Gewohnheiten, wie sie über gesellschaftliche Institutionen hergestellt und vermittelt werden, Einschränkungen auferlegt sind, die das Verhalten mit einer gewissen Wahrscheinlichkeit antizipierbar, das heißt vorhersagbar machen. Und schließlich ist die Vorhersagbarkeit menschlichen Verhaltens geradezu Voraussetzung und Notwendigkeit für einen reibungslosen gesellschaftlichen Ablauf.

Seite 136

Durch das Maschinenhafte in uns unterscheiden wir uns *als Menschen* vom Tier.

Seite 139

5 Körper und Technik

Der Mensch scheint an seinem selbst gesteckten Ziel angelangt zu sein. Zumindest in der wissenschaftlichen Bestimmung ist es ihm gelungen, die Technik sowie die Welt überhaupt und damit auch sich selbst, zu entmaterialisieren. Der Mensch ist – wie die Technik, wie die ursprüngliche und die soziale Natur – zu einem bloßen Informationsfluß oder Sprachspiel geworden. Die Erkenntnisse über das Verhältnis von Mensch und Technik werden nicht länger aus der Anschauung der Empirie gewonnen. Die Begriffe verweisen nicht mehr auf Empirisches, sie haben sich von der Materie gelöst. Sie sind zu einem Diskurs geworden, zum bloßen Daten-, Zeichen-, Informationsverkehr. Und diese Neudefinition von Mensch und Maschine wird, wie wir gesehen haben – auf die Geschichte der Technik und des Menschen ausgedehnt, projiziert.

---

[42] Ein lesenswerter Zeitungsartikel: Die Simulanten – Ein Gespräch mit John R. Searle über das Bewusstsein von Maschinen und den Film "AI – Künstliche Intelligenz", Das Gespräch führte Christine Brinck; DIE ZEIT Nr. 39, 20. September 2001, Seite 44; http://www.zeit.de/2001/39/Media/print_200139_p-searle_intervi.html

Im folgenden werde ich jedoch zeigen, dass Technik zwar dem Menschen nichts äußerliches ist, das heißt, dass das Menschsein auch mit der Technik zusammenhängt, ebenso mit der Sprache. Aber nicht nur. Der Mensch ist immer auch Körper. Wenngleich mit dem Beginn der Antike ein kleiner Kulturkreis alles daran setzt, seinen Körper, wie die Natur überhaupt, unter Kontrolle zu bekommen. Dies geschieht einmal mit der Ablösung der Sprache vom Körper in die lineare Symbolschrift. Des weiteren in der zunehmenden Ablösung der technischen Funktionslogik von der Determinierung der Materie. Zunächst zieht dies eine Eliminierung der organischen, aber tendenziell auch der unorganischen Materie nach sich. Wobei der Mensch als immaterielle Instanz bestimmt, und sein Körper in der Logik der jeweils vorherrschenden Technik begriffen und zugerichtet wird. In der Antike ist er Werkzeug. Dann, unter dem Eindruck der sich selbst bewegenden Maschine folgt das Körper-Bild der Bewegung der Uhr, schließlich der Wärmekraftmaschine (als Energiefluß) und zuletzt der Funktionslogik des Computers. Im letzteren fallen, da nun die Maschine von der Materie befreit ist, Mensch und Technik wieder zusammen.

Seite 157:
Die Herrschaft des Denkens über den Körper, das Organische drückt sich ebenso in der in dieser Zeit entstandenen linearen Symbolschrift aus. Denn durch sie verändert sich das Verhältnis von Körper und Denken, und das Verhältnis von Denken und Sprache entscheidend. *Mit dieser Schrift löst sich das Denken vom Sprechen*, vom Körper. Damit entsteht ein Denken, ein Denksystem als Zeichensystem, das sich – zwar noch nicht in seiner Entstehung, aber in der Vermittlung, in der Weitergabe – vom Einfluß des Sprechenden, vom Einfluß des Organischen gelöst hat. Mit der linearen Symbolschrift haben sich die Wörter vom Leib und der ihn umgebenden Natur gelöst; oder sie konnten sich im weiteren lösen. Denn die Schrift ermöglicht die Schaffung einer Wirklichkeit, einer Erfahrung der Welt als bloß geistige. Das Lesen, die visuell-geistige Aufnahme der Zeichen tritt an die Stelle der Erfahrung als sinnliche Wahrnehmung und Handlung des Menschen als Einheit von Denken und Körper. Unabhängig von der leiblichen Präsenz desjenigen, der geschrieben hat, kann dessen Wissen von jedem, der die Schrift lesen kann, zu jeder Zeit erfahren werden. Von der Antike an hat sich die menschliche Erfahrung zunehmend auf das Lesen von Schriftzeichen reduziert. Die menschliche Welt wird zu dem, was in einer bloß geistigen Erfahrung über sie aufgeschrieben werden kann, was in den Vorstellungen des Menschen entsteht, was im schriftlichen Diskurs über sie festgelegt wird.

Seite 167
Kant: Der Mensch wird erst durch die *Erziehung* zum Menschen. In der Verdrängung und Zurichtung des Leibes und der damit verknüpften Sinnes- und Geistesleistungen. Durch den Erwerb und durch die Produktion des Begriffssystems. In der Ausbildung einer von der Materie befreiten, bloßen Vernunft liegt die wahre Größe des Menschen.

Seite 189
Die Androidin wird nur über den Geist verfügen, den Lord Ewald ihr zugesteht, versichert ihm Edison: „Mit der zukünftigen Alicia ..., der wahren“, werden Sie „das Wort, das Sie erwarten, ... auch vernehmen. Ihr ‚Bewußtsein‘ wird nicht länger die Verneinung Ihres eigenen sein, sondern den Schein derjenigen Seele tragen, die Ihrer Stimmung gerade am besten entspricht. Ihre eigene Liebe werden Sie in ihr widerspiegeln können, ohne diesmal eine Enttäuschung zu erleben. Nie werden Ihre Worte mit Ihrer Hoffnung in Widerspruch stehen, sondern stets mit Ihrer eigenen Begeisterung im Einklang sein. Hier werden Sie wenigstens nie, wie mit der lebenden, Mißverständnissen begegnen ... Ja, es wird gar nicht mehr nötig sein, dass Sie reden. Denn ihre Worte werden stets die Antwort auf Ihre Gedanken wie auf Ihr Schweigen sein.“

Seite 191
Die Problemstellung des Imitationsspiels {Bezug ist der Turing-Test} macht nicht nur den Vorgang des Erkennens abstrakt, sondern erlaubt Turing sowohl die Maschine als auch den Menschen ausschließlich über abstrakte Merkmalszuweisungen zu identifizieren. Indem er jegliche körperliche Identifizierung ausschließt, schafft Turing sich die Basis, Mensch *und* Maschine als abstrakte Zustände, als bloße Vorstellung zu beschreiben, zu bestimmen. In der Beschreibung von Mensch und Maschine *verschwindet* folglich die *Differenz von Körper und Denken*. Beides fällt unter die *Einheit des bloßen Denkens*.

Seite 193
Denn „wir bewegen uns nur mehr in einer Welt von Modellen, in welcher Modelle entscheiden, was ein Modell ist, ob ein Modell das Modell innerer oder äußerer Vorgänge ist, wo die Vorgänge aufhören, Vorgänge zu sein, und beginnen, Modell zu werden, ob es Sinn hat, von Vorgängen zu sprechen, die nicht Modell sind, ob ein Zuordnungsmechanismus, der ein Modell auf ein anderes bezieht, selbst ein Modell ist ...“ (Zitat aus: Oswald Wiener: Turing Test. Vom dialektischen zum binären Denken. In: Kursbuch 75, 1984, Seite 24

Seite 208f
Und die Tatsache, dass mit dieser Bestimmung die Systeme als lebendig gelten, die sich selbst erzeugen können, bedeutet: jegliche Dinge, also auch oder vor allem die vom Menschen erzeugten können als lebendige Systeme begriffen, erkannt werden. Also sowohl biotechnische als auch informationstechnische als auch soziale Systeme.

Seite 211
Nicht mehr der Körper, das Empfinden der Sinne bestimmt die Beurteilung, sondern allein die Mittel der Kalkulation.

DigitaLiberty

Return-Path: <listserv@cpsr.org>
Received: from snyside.sunnyside.com by tcs.inf.tu-dresden.de (4.1/SMI-4.1)
id AA02739; Sat, 10 Dec 94 04:54:43 +0100
Errors-To: cpsr-announce-errors@Sunnyside.COM
Received: (from al@localhost) by snyside.sunnyside.com (8.6.9/8.6.6.Beta9) id QAA14318; Fri, 9 Dec 1994 16:35:47 -0800
From: email list server <listserv@Sunnyside.COM>
Message-Id: <199412100035.QAA14318@snyside.sunnyside.com>
Errors-To: cpsr-announce-errors@Sunnyside.COM
Reply-To: listserv@Sunnyside.COM
Sender: cpsr-announce@Sunnyside.COM
Precedence: bulk
To: cpsr-announce@sunnyside.com
X-Mailer: Sunnyside List-serv 1.0
Date: Tue, 6 Dec 1994 18:38:13 -0800
Subject: DigitaLiberty

Friends of Liberty,

It is becoming increasingly apparent that the arrival of cyberspace is destined to engender a fundamental discontinuity in the course of human relations. This is a source of great optimism and opportunity for those of us who believe in freedom.

Many of you who participate in the lively debates that take place in these forums have seen a number of activist organizations spring up claiming to represent the cause of freedom. And if you are like me you have cheered these groups on only to watch them get bogged down in a quagmire of realpolitics.

It is a sad fact that the beast in Washington has evolved into a self-perpetuating engine expert at co-opting the principles of even the most ardent reformers. Slowly but surely all those who engage the system are ultimately absorbed into the mainstream miasma of majoritarianism. For example, what can be more discouraging than watching an organization that started out as a cyber-civil liberties group shift its focus to creating new forms of government entitlements while endorsing intrusive wiretap legislation because they didn't want to jeopardize their influence and prestige amongst the Washington power elite?

Some of us believe we can seek ultimate redress at the polls. Many pundits have declared our recent national elections a watershed in politics, a turning point that represents the high water mark of big government.
Nonsense. The names have changed, the chairs have been rearranged, but the game remains the same. The so-called "choices" we are presented with are false, hardly better than the mock one-party elections held by failed totalitarian regimes. There must be a better way.

I would like to announce the formation of a new group - DigitaLiberty - that has chosen a different path. We intend to bypass the existing political process. We reject consensus building based on the calculus of compromise.
Instead we plan to leave the past behind, much as our pioneering forefathers did when they set out to settle new lands. It is our mission to create the basis for a different kind of society. If you would like to join us I invite you to read the information below.

Yours in freedom,

Bill Frezza
Co-founder, DigitaLiberty
December 6, 1994

What is DigitaLiberty?

DigitaLiberty is an advocacy group dedicated to the principled defense of freedom in cyberspace. We intend to conduct this defense not by engaging in traditional power politics but by setting an active, persuasive example - creating tangible opportunities for others to join us as we construct new global communities.

We believe deeply in free markets and free minds and are convinced that we can construct a domain in which the uncoerced choices of individuals supplant the social compact politics of the tyranny of the majority.

Is DigitaLiberty a political party or a lobbying group?

Neither.

DigitaLiberty does not seek to educate or influence politicians in the hope of obtaining legislation favorable to our constituents. We plan to make politicians and legislators irrelevant to the future of network based commerce, education, leisure, and social intercourse.

DigitaLiberty does not seek to persuade a majority of the electorate to adopt views which can then be forced upon the minority. We hope to make majoritarianism irrelevant. We invite only like minded individuals to help us build the future according to our uncompromised shared values.

What do you hope to accomplish?

DigitaLiberty is not hopeful that widespread freedom will come to the physical world, at least not in our lifetime. Too many constituencies depend upon the largess and redistributive power of national governments and therefore oppose freedom and the individual responsibility it entails. But we do believe that liberty can and will prevail in the virtual domains we are building on the net and that national governments will be powerless to stop us. We believe that cyberspace will transcend national borders, national cultures, and national economies. We believe that no one will hold sovereignty over this new realm because coercive force is impotent in cyberspace.

In keeping with the self-organizing nature of on-line societies we believe we will chose to invent new institutions to serve our varied economic and social purposes. DigitaLiberty intends to be in the forefront of the discovery and construction of these institutions.

But what about the construction of the "Information Superhighway"?

The fabric of cyberspace is rapidly being built by all manner of entities espousing the full range of political and economic philosophies. While political activity can certainly accelerate or retard the growth of the net in various places and times it cannot stop it nor can it effectively control how the net will be used.

Our focus is not on the institutions that can and will impact the building of the physical "information highway" but on those that will shape life on the net as an ever increasing portion of our productive activities move there.

What makes you think cyberspace will be so different?

The United States of America was the only country in history ever to be built upon an idea. Unfortunately, this idea was lost as we slowly traded away our liberties in exchange for the false promise of security.

DigitaLiberty believes that technology can set us free. The economies of the developed world are now making a major transition from an industrial base to an information base. As they do, the science of cryptology will finally and forever guarantee the unbreachable right of privacy, protecting individuals, groups, and corporations from the prying eyes and grasping hands of

sovereigns. We will all be free to conduct our lives, and most importantly our economic relations, as we each see fit.

Cyberspace is also infinitely extensible. There will be no brutal competition for lebensraum. Multiple virtual communities can exist side by side and without destructive conflict, each organized according to the principles of their members. We seek only to build one such community, a community based on individual liberty. Others are free to build communities based on other principles, even diametrically opposed principles. But they must do so without our coerced assistance.

Effective communities will thrive and grow. Dysfunctional communities will wither and die. And for the first time in human history, rapacious societies will no longer have the power to make war on their neighbors nor can bankrupt communities take their neighbors down with them.

What does this have to do with my real life? I can't eat data. I don't live in a computer.

Yes, but imagine the ultimate impact of mankind's transition from an agrarian economy to an industrial economy to an information economy. Our founding fathers would have consider anyone insane who predicted that a nation of 250 million could feed itself with fewer than 3% of its citizens involved in agriculture. Similarly, economist and politicians trapped in the policies of the past lament our move from a manufacturing economy to a knowledge worker and service based economy. We see this as a cause to rejoice.

The day will come when fewer than 5% of the citizens of a nation of 1 billion will be involved in manufacturing - if we still bother calling geographically defined entities "nations". What will the rest of us be doing? We will be providing each other with an exploding array of services and we will be creating, consuming, and exchanging information. Most of this will occur entirely within or be mediated at least in part by our activities in cyberspace.

Many of us will earn a very good living on the net. Our race, our religion, our gender, our age, our physical appearance and limitations will all be irrelevant and undetectable. Hard working individuals from underdeveloped nations who in the past might have been forced to emigrate in search of economic freedom and opportunity can now build productive lives in cyberspace. And much if not all of the wealth we create that we do not transform into visible physical assets will be ours to keep and use, beyond the grasp of sovereigns.

What is the purpose of this forum?

The DigitaLiberty Forum is a place where like minded individuals can share their views, observations, and strategies related to the development of virtual communities based on freedom. It is a place where people can exchange information and advice about how they have developed extra-territorial business and social relationships - away from the influence and outside the jurisdiction of governments. It is a forum for the posting of essays, questions, and ideas on the topic of liberty. It is a place where we can meet and debate the forms that our new institutions might take and discuss the practical problems and responsibilities that freedom entail.

In time as our technology matures some of us will move on to more ambitious projects, launch other programs, and begin our virtual migration from the swamp of coerced collectivism. Best of all, there will be no need to physically move to 'Galt's Gulch' or escape to a floating 'Freedonia'. We

can all participate in this exodus without hastily quitting our jobs or disrupting our lives. And as a larger and larger portion of our economic and social activities move onto the net we will create a new society, open to all with the will to enter. This new world will be interleaved with the physical world in which we now live and yet will be separate. And free.

Join us as we begin the journey.

Who can join DigitaLiberty?

The DigitaLiberty Forum is open to anyone that can honestly answer yes to the following two questions:

1) I renounce the use of coercive force as a tool of social or economic policy.

2) I do not derive the majority of my income from funds taken from taxpayers.

How do I join DigitaLiberty?

If you qualify, send a message to DigitaLiberty-request@phantom.com with the words "SUBSCRIBE" in the subject line and the message body as follows

SUBSCRIBE DigitaLiberty <your name>

And welcome to the future.

--- CPSR ANNOUNCE LIST END ---

To alter or end your subscription to this mailing list, write to listserv@cpsr.org. For general information send the message:

HELP

To unsubscribe, send the message:

UNSUBSCRIBE CPSR-ANNOUNCE

You need to do this from the same machine you subscribed from. In both cases, leave the subject blank, or at least not resembling an error message.

Identität im Internet

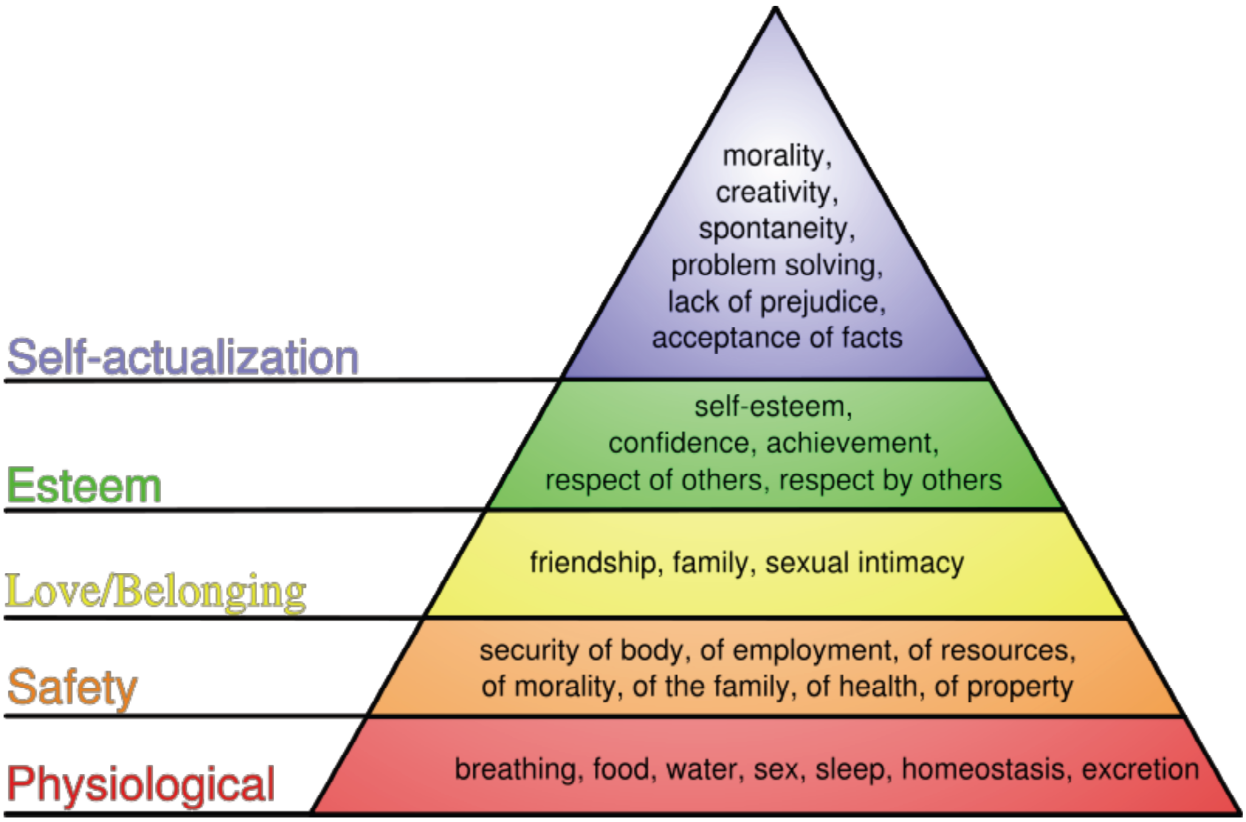
Sherry Turkle, die Autorin des Klassikers „Die Wunschmaschine: Vom Entstehen der Computerkultur“ (engl. Original „The second self“, erschienen 1984) hat 1995 mit „Life on the Screen“ (dt. Übersetzung 1998: „Leben im Netz – Identität in Zeiten des Internet“) ein Buch vorgelegt, in dem einerseits das Material ihres leider vergriffenen Klassikers von 1984 nochmals kurz gebracht wird (Wie gehen Menschen mit isolierten Rechnern um? Sehen sie sie als Partner oder Sklaven? Maschine oder Lebewesen?). Andererseits wird auf den Umgang von Menschen mit Rechnernetzen eingegangen: Wie agieren Menschen in Multi-User Domains (MUDs)? Was (er)leben sie dort und was bedeutet dies für sie?

Einem ähnlichen Thema ist das Heft 2/99 (Juni 1999) der FIFF-Kommunikation gewidmet: Virtuelle Identität in der sozialen Gemeinschaft.

Die Maslowsche Bedürfnispyramide (Maslow's hierarchy of needs)

... ist eine Hilfe zur Problempriorisierung und –einordnung

http://en.wikipedia.org/wiki/Maslow%27s_hierarchy_of_needs
http://chiron.valdosta.edu/whuitt/col/regsys/maslow.html



homeostasis = Gleichgewicht der Körperfunktionen; excretion = Absonderung, Ausscheidung

Bezogen of Bedürfnisse bzgl. Datenverarbeitung, entwickelt David Chaum hieraus folgende Bedürfnispyramide (Chaum’s Hierarchy of IT Needs):

Self-Worth – relation to: artificial intelligence, etc.
Cyber Sovereignity –privacy, free expression, transparency
Interaction – communication, exploration, commerce
Security – stable, robustness, un-hacked
Processing – storage, interface, crunching

Maslow's Hierarchy of Needs

Citation: Huitt, W. (2004). Maslow's hierarchy of needs. *Educational Psychology Interactive*. Valdosta, GA: Valdosta State University. Retrieved [date] from, http://chiron.valdosta.edu/whuitt/col/regsys/maslow.html.

Abraham Maslow (1954) attempted to synthesize a large body of research related to human motivation. Prior to Maslow, researchers generally focused separately on such factors as biology, achievement, or power to explain what energizes, directs, and sustains human behavior. Maslow

posited a hierarchy of human needs based on two groupings: deficiency needs and growth needs. Within the deficiency needs, each lower need must be met before moving to the next higher level. Once each of these needs has been satisfied, if at some future time a deficiency is detected, the individual will act to remove the deficiency. The first four levels are:

1) Physiological: hunger, thirst, bodily comforts, etc.;

2) Safety/security: out of danger;

3) Belonginess and Love: affiliate with others, be accepted; and

4) Esteem: to achieve, be competent, gain approval and recognition.

According to Maslow, an individual is ready to act upon the growth needs if and only if the deficiency needs are met. Maslow's initial conceptualization included only one growth need--self-actualization. Self-actualized people are characterized by: 1) being problem-focused; 2) incorporating an ongoing freshness of appreciation of life; 3) a concern about personal growth; and 4) the ability to have peak experiences. Maslow later differentiated the growth need of self-actualization, specifically naming two lower-level growth needs prior to general level of self-actualization (Maslow & Lowery, 1998) and one beyond that level (Maslow, 1971). They are:

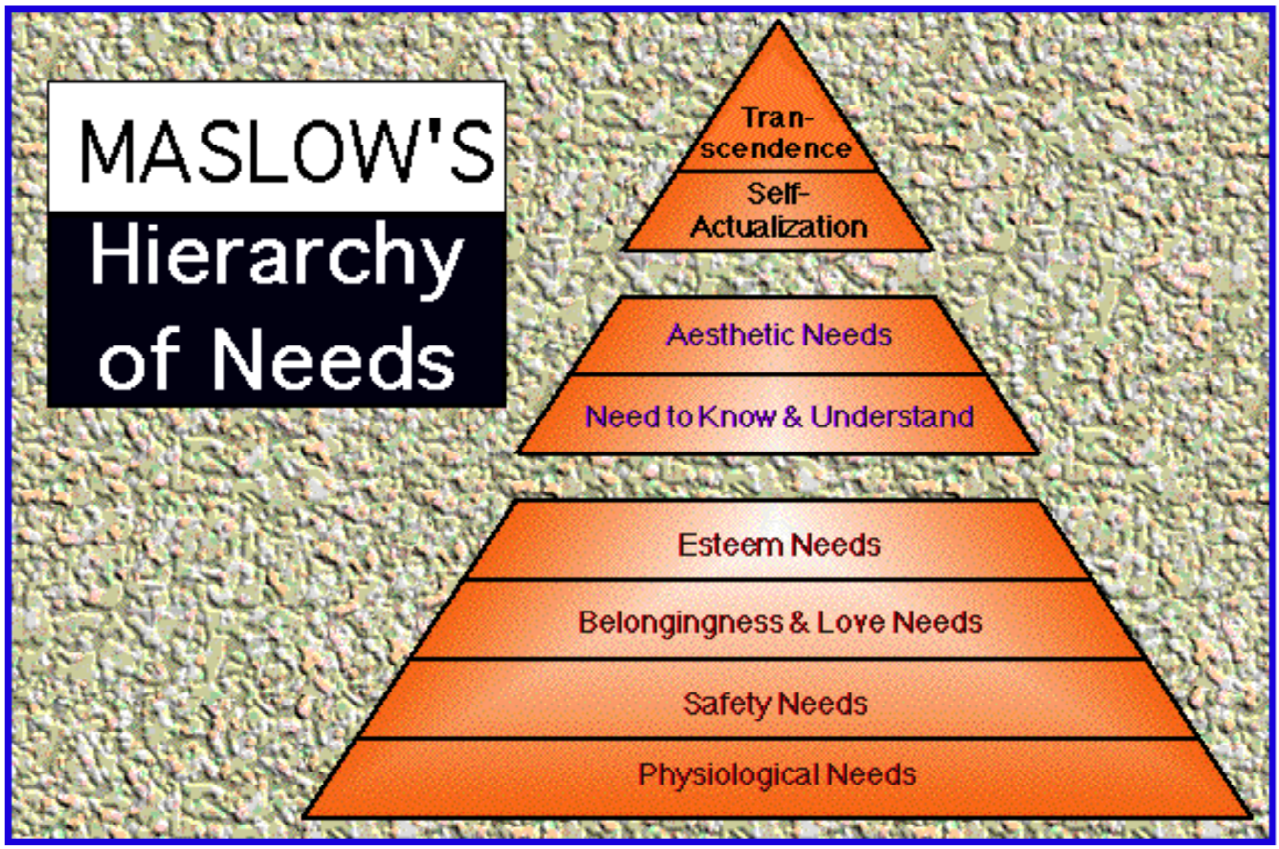
5) Cognitive: to know, to understand, and explore;

6) Aesthetic: symmetry, order, and beauty;

7) Self-actualization: to find self-fulfillment and realize one's potential; and

8) Self-transcendence: to connect to something beyond the ego or to help others find self-fulfillment and realize their potential.

Maslow's basic position is that as one becomes more self-actualized and self-transcendent, one becomes more wise (develops wisdom) and automatically knows what to do in a wide variety of situations.


MASLOW'S
Hierarchy
of Needs
Tran-
scendence
Self-
Actualization
Aesthetic Needs
Need to Know & Understand
Esteem Needs
Belongingness & Love Needs
Safety Needs
Physiological Needs

Zukunftsdiskussion

Einerseits sollte das präsentierte Material *jeden persönlich* anregen, sich zu überlegen, was sie/er individuell im Bereich Informatik und Gesellschaft tun kann und sollte.

Andererseits sollten *InformatikerInnen auch als gesellschaftliche Gruppe* überlegen, was sie kollektiv tun können und sollen.

Eine sinnvolle Strukturierung der Diskussion scheint mir zu sein, zunächst zu klären, was sozusagen von allein kommt. Wird dies Kommende positiv eingeschätzt, braucht diesbezüglich niemand eine außerordentliche Initiative zu ergreifen. Es genügt, einfach mitzuwirken.

Vermutlich bleiben Defizite, d.h. es gibt weitere Dinge, die wir uns wünschen würden, die aber nicht „von allein“ kommen. Hier ist es ggf. nötig, die Initiative zu ergreifen und sich ggf. außerordentlich zu engagieren.

Operationalisiert wird dies durch die Frage: Was können wir wie beeinflussen?

Am Ende des ersten Durchlaufs der Vorlesung an der TU Dresden (Juli 1994) habe ich mir 6 Gebiete herausgegriffen und versucht, für sie die obigen Fragen zu beantworten:

Was kommt von alleine?

1. Mäßig fehlertolerante und für den Systembetreiber, nicht aber für den Systembenutzer sichere IT-Systeme;
2. Zunehmende Durchdringung und damit auch Abhängigkeit fast aller Bereiche des Lebens vom Funktionieren von IT-Systemen, d.h. zunehmende Verletzlichkeit der Gesellschaft;
3. Ergonomische Benutzungsschnittstellen;
4. Produkthaftung auch für IT;
5. Allgemeine, freiwillige berufsethische Kodizes;
6. Europäische Harmonisierung des Datenschutzrechts auf mittlerem bis hohem Niveau

Was würden wir uns wünschen?

1. Hochgradig fehlertolerante und für alle Beteiligten sichere IT-Systeme
2. Einerseits weniger kritische Anwendungen der IT, damit die Abhängigkeit nicht so gravierend wird; andererseits hochgradig gesicherte, z.B. redundante Systeme und Strukturen bei allen informationstechnischen Infrastrukturen;
3. Auch behindertengerechte Benutzungsschnittstellen;
4. Korrekte und sozial akzeptable IT-Systeme
5. Allgemeine und spezielle obligatorische berufsethische Kodizes
6. Europäische Harmonisierung des Datenschutzrechts auf sehr hohem, einer Informationsgesellschaft langfristig angemessenem Niveau sowie Ausdehnung auf nicht personenbezogene Daten (frei nach Adalbert Podlech: vom Individualdatenschutz zum Systemdatenschutz)

Was können wir wie beeinflussen?

1. Schwächen und Verbesserungsmöglichkeiten von IT-Systemen auch bzgl. Fehlertoleranz und Sicherheit öffentlich bekannt machen;
2. Auf die vergleichsweise große Verletzlichkeit der informationstechnischen Infrastrukturen hinweisen, diese zu Verringern trachten und, solange dies noch nicht geschehen ist, das Schadenspotential der auf ihnen realisierten Dienste begrenzen;
3. Benutzungsschnittstellen auch behindertengerecht gestalten;
4. Methoden zur Spezifikation und zum Korrektheitsnachweis (unter Einschluß von Fehlertoleranz und Sicherheit) erforschen, lehren, lernen, fordern und auch selbst anwenden;
5. Inhalt der allgemeinen und speziellen obligatorischen berufsethischen Kodizes
6. Expertenhearings in Brüssel zum Thema Datenschutz aus technischer Sicht

Wie würden Sie diese Fragen aus heutiger Sicht beantworten? Und welche Gebiete wären Ihnen wichtig?

Literaturverzeichnis

AJGP_93 Ronald E. Anderson, Deborah G. Johnson, Donald Gotterbarn, Judith Perrolle: Using the ACM Code of Ethics in Decision Making; Communications of the ACM 36/2 (1993) 98-107.

Chau2_90 David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, Sydney, Australia, January 1990, LNCS 453, Springer-Verlag, Berlin 1990, 246-264.

ClPf_91 Wolfgang Clesle, Andreas Pfitzmann: Rechnerkonzept mit digital signierten Schnittstellenprotokollen erlaubt individuelle Verantwortungszuweisung; Datenschutz-Berater 14/8-9 (1991) 8-38.

Coy_89 Wolfgang Coy: Brauchen wir eine Theorie der Informatik? Informatik-Spektrum 12/5 (1989) 256-266.

Echt_90 Klaus Echtle: Fehlertoleranzverfahren; Studienreihe Informatik, Springer-Verlag, Heidelberg 1990.

Hoch_87 Rolf Hochhuth: Alan Turing – Erzählung; Rowohlt, Reinbek 1987.

IFIP_92 IFIP-WG9.2 On Behalf of IFIP-TC9: Ethics of Computing: Information Technology and Responsibility; To Promote Discussion Inside the IFIP National Societies; Madrid, september 1992.

Kopp_93 Ferdinand Kopp: Der EG-Richtlinienvorschlag zum Datenschutz in Europa; Geänderter Vorschlag der EG-Kommission für "Eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"; Datenschutz und Datensicherung DuD 17/1 (1993) 11-17.

Parn1_94 D. L. Parnas: Professional Responsibilities of Software Engineers; Klaus Brunnstein, Eckart Raubold: Technology and Foundations; IFIP 13th World Computer Congress 94, Volume 2, Elsevier Science B.V., Amsterdam 1994, 332-339.

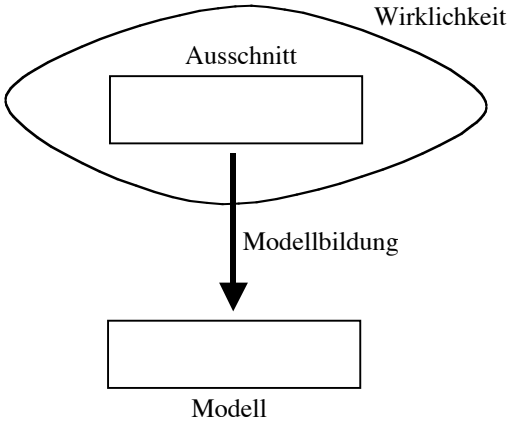
Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990.

Anhänge

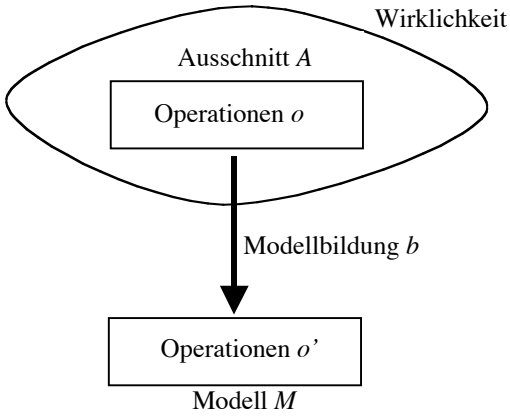
Die prinzipielle Fehlerhaftigkeit[43]

Fehlerhaftigkeit menschlichen Modellierens und Gestaltens

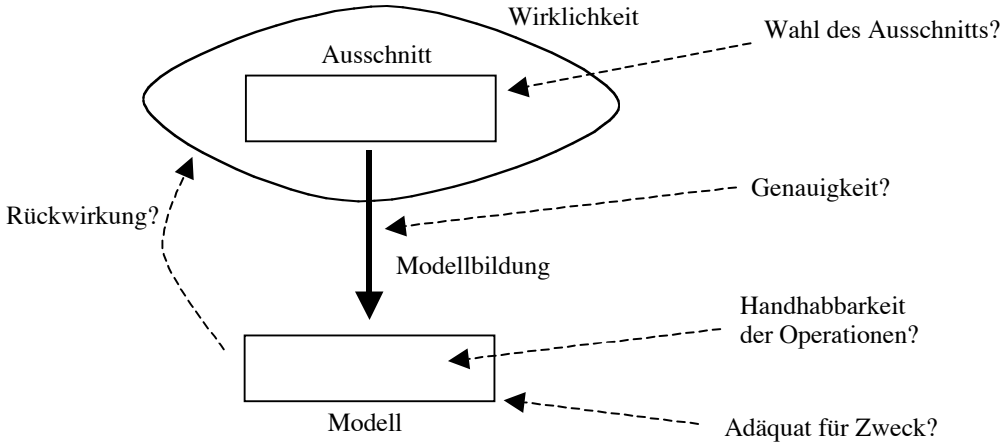
Modelle stellen prinzipiell nur einen ungenau abgebildeten Ausschnitt der Wirklichkeit dar. Sie sind bestenfalls adäquat für einen bestimmten Zweck, dafür aber durch den Menschen oder zumindest rechnergestützt handhabbar. Könnte man bei der Modellbildung die gesamte Wirklichkeit in voller Genauigkeit berücksichtigen, erhielte man ein für alles adäquates Modell, was aber nichts nützen würde, weil es selbst rechnergestützt nicht mehr handhabbar wäre. Bei der Modellbildung geht also zwangsläufig Information verloren, die bei Benutzung des Modells zu Fehlern führen kann.



Bei der Bildung eines Modells müssen Operationen in der Wirklichkeit auf Operationen im Modell abgebildet werden. Diese Abbildung *b* sollte ein Isomorphismus sein, d.h. eine Operation im Modell entspricht genau einer Operation in der Wirklichkeit und umgekehrt. Auch diese Abbildung muß gerade so genau erfolgen, dass das Modell seinen Zweck erfüllt und trotzdem handhabbar bleibt.



Die wichtigsten Parameter bei der Modellbildung sind also die Wahl des Ausschnitts aus der Wirklichkeit und die Genauigkeit der Modellierung. Da man vor der Modellbildung noch nicht weiß, wie adäquat und handhabbar das Modell wird, sind oft mehrere Iterationen nötig, um ein für den vorgegebenen Zweck ausreichend adäquates und handhabbares Modell zu erhalten.



Ein Modell ist seinerseits ein Teil der Wirklichkeit, wirkt also auf sie ein und ändert damit oftmals den ihm vorgegebenen Zweck. Außerdem kann sich die Wirklichkeit selbst jederzeit ändern. Momentan adäquate Modelle können also zum nächsten Zeitpunkt schon wieder inadäquat sein. Dies wird oft zu spät erkannt, wenn erstmal ein gutes Modell vorhanden ist bzw. war. Die Modellbildung muß dann wiederholt werden, wobei man zweckmäßigerweise das alte Modell als Grundlage benutzt.

Modelle als Welterklärungs- und Herrschaftsinstrument

Modelle können durch bewussten Einbau von Fehlern oder Ungenauigkeiten als Mittel zur Machtausübung benutzt werden. Urteile über die Adäquatheit von Modellen hängen i.d.R. von den Interessen derer ab, die sie beurteilen.

Für den Informatiker bedeutet das, dass (v.a. angewandte) Informatik durchaus nicht interessen- und wertfrei ist. Dem Informatiker obliegt vielmehr, wie jedem anderen Wissenschaftler auch, die Verantwortung, die Interessen und Werte offenzulegen, so dass demokratische Prozesse nach und nach für global adäquatere Modelle sorgen können.

Fehlerhaftigkeit physischer Geräte

Beim Entwurf eines Gerätes sind stets Menschen am Werk und benutzen in den meisten Fällen Werkzeuge, die ihrerseits von Menschen geschaffen wurden. Da Menschen nie hundertprozentig fehlerfrei arbeiten, können sowohl die Konstrukteure Fehler einbauen als auch die Werkzeuge bereits fehlerhaft sein. Im Fall der Werkzeuge lässt sich die Rekursion fortsetzen, d.h. auch um sie zu bauen, wurden Werkzeuge benutzt, die fehlerhaft sein konnten, usw. Saboteure können sich diese Rekursion sehr gut zunutze machen, indem sie transitive trojanische Pferde in die Werkzeuge einbauen.

Bei der Produktion der Geräte können außerdem noch Fehler auftreten, und es können Geräte durch Alterung fehlerhaft werden. Zudem können durch Sabotage verschiedenster Art Geräte unbrauchbar gemacht werden, z.B. zerstört ein ausreichend starker elektromagnetischer Impuls alle elektronischen Geräte, die nicht sicher genug verbunkert bzw. abgeschirmt sind.

---

[43] **Dokumentation der Vorlesung im SoSe 2001 durch Dietrich Clauß <dc2@clauss.dyndns.org>**

Planvoller Umgang mit Fehlern

Beachtet man Murphys Gesetz („If anything can go wrong, it will!“), lassen sich trotz der oben beschriebenen Fehlermöglichkeiten funktionierende Systeme aufbauen. Wichtig ist eine möglichst hohe Fehlertoleranz oder sogar Fehlerfreundlichkeit.

Man sollte nie einem einzigen Menschen oder einem Gerät vollständig vertrauen, sondern verteilte Systeme benutzen, deren Komponenten sich gegenseitig kontrollieren. Im Bereich der IT-Systeme erreicht man das, indem man dezentrale Kontroll- und Implementierungsstrukturen benutzt (z.B. mittels vernetzter Rechner), die auch beim Ausfall einzelner Komponenten noch funktionieren und diesen Ausfall sogar anzeigen.

Untersuchungen zur Verletzlichkeit einer vernetzen Gesellschaft

Von Ulrich Pordesch und Alexander Roßnagel

Die Verletzlichkeit der Gesellschaft wird im diesem Beitrag als ein Kriterium zur Analyse und Bewertung künftiger Technikfolgen beschrieben. Ihre Untersuchung zielt letztlich auf die Verhinderung möglicher negativer Folgen durch die Mobilisierung von Gegensteuerung sowie auf das Aufzeigen von Alternativen, die die Verletzlichkeit reduzieren (Kap. 1). Die bisher umfassendste Verletzlichkeitsuntersuchung liegt bereits acht Jahre zurück. Am Beispiel der Telekommunikation werden wichtige Ergebnisse dieser Untersuchung referiert (Kap. 2) und mit den zwischenzeitlich eingetretenen Änderungen in den gesellschaftlichen Rahmenbedingungen der Nutzung von Telekommunikationstechnik konfrontiert (Kap. 3). Als Ergebnis dieser Überprüfung können neue Schwerpunktsetzungen und Hypothesen für künftige Verletzlichkeitsuntersuchungen festgehalten werden. Diese werden am Beispiel des Internet, das von vielen als Modellfall für die künftige Entwicklungen der Telekommunikation angesehen wird, näher untersucht. Hierdurch wird zugleich das Design einer Studie zur Entwicklung der Verletzlichkeit einer durch das Internet vernetzten Gesellschaft vorgestellt (Kap. 4).

1. Das Kriterium Verletzlichkeit

Die Verletzlichkeit der Gesellschaft soll durch den Einsatz neuer Techniken nicht erhöht, sondern vermindert werden! Diese Forderung verfügt über eine hohe Konsensfähigkeit und kann zur Grundlage der Analyse, Bewertung und Gestaltung von Informations- und Kommunikationstechniken dienen (Roßnagel u.a. 1990a). Zur Umsetzung dieser Forderung sind Untersuchungen notwendig,

- welche Entwicklungsalternativen sich in der Nutzung neuer Techniken mit Blick auf ihr Verletzlichkeitspotential ergeben,
- wie diese zu bewerten sind und
- welche Möglichkeiten sich bieten, die Verletzlichkeit durch Maßnahmen - vor allem der Technikgestaltung - zu verringern.

Wie eine solche Untersuchung für die Zukunft einer vernetzten Gesellschaft durchgeführt werden könnte, soll im folgenden am Beispiel der Telekommunikation angedeutet werden.

Das Problem der Verletzlichkeit der Gesellschaft durch Telekommunikation entsteht vor allem dadurch, dass gesellschaftliche Funktionen von Menschen auf Techniksysteme übertragen werden. In unserem Fall werden durch diesen Schritt Informationsverarbeitung und Kommunikation vom Funktionieren einer Technik abhängig, auf die sich die Menschen verlassen. Im Vertrauen auf die Technik erhöhen sie deren Leistungsfähigkeit - und damit zugleich das Schadenspotential.

Verletzlichkeit bezeichnet die Möglichkeit großer Schäden für Individuen, Gruppen, Organisationen und für die Gesellschaft insgesamt. Unter diesem Blickwinkel gilt das Interesse nicht dem technischen System als solchem, sondern den sozialen Folgewirkungen seines Ausfalls oder seiner Störung. Die Untersuchung von Risiken und Gestaltungsvorschlägen gilt daher nicht nur der Sicherheit von Geräten und Systemen, sondern vor allem der Verhinderung großer Schäden für die Gesellschaft oder für einzelne. Die auf die Techniksysteme bezogene Fragestellung soll in Abgrenzung zur Verletzlichkeit der Gesellschaft als Verwundbarkeit der Techniksysteme bezeichnet werden.

Für eine Verletzlichkeitsuntersuchung zu prüfen sind also die zu erwartende Abhängigkeit einzelner oder der Gesellschaft von bestimmten Techniksystemen der Telekommunikation, das mögliche Schadensausmaß eines Versagens der Technik oder eines gelungenen Mißbrauchs, die Möglichkeiten, das potentielle Schadensausmaß zu vermindern oder Mißbrauchsmöglichkeiten auszuschließen, aber auch die sozial begründete Verlässlichkeit solcher Sicherungsmaßnahmen und ihre sozialen Auswirkungen.

Zur Beurteilung der Verletzlichkeit einer vernetzten Gesellschaft sind danach folgende Untersuchungsschritte notwendig:

Als Ausgangspunkt der Untersuchung sind die *in der Zukunft* **möglichen Anwendungen** der Telekommunikationstechnik auf ihr Verletzlichkeitspotential abzuschätzen. Das Ziel dieser Abschätzung ist allerdings nicht, die Zukunft vorherzusagen, sondern heutige Zukunftswünsche zur Fortentwicklung der Telekommunikation kritisch zu überprüfen. Sofern irgendmöglich sollen hierzu alternative Entwicklungsmöglichkeiten untersucht werden. Denn Kriterien der Technikbewertung und Vorschläge zur Technikgestaltung können politische Relevanz nur in geschichtlichen Verzweigungssituationen gewinnen.

Die künftigen Anwendungen bestimmen den Rahmen für mögliche Aktionen und Sicherungsmaßnahmen. Aus ihnen ist vor allem der **virtuelle Schaden** eines Fehlers oder Mißbrauchs der Telekommunikation abzuleiten. Als virtuell wird ein Schaden oder eine Wahrscheinlichkeit bezeichnet, die als Ergebnis eines analytischen Zwischenschritts zu erwarten wären, wenn keine besonderen Gegenmaßnahmen ergriffen werden. Der virtuelle Schaden ergibt sich aus den negativen gesellschaftlichen Auswirkungen, wenn eine gesellschaftliche Funktion, die dem Techniksystem übertragen wurde, ausfällt oder gestört wird. Das inhärente Schadenspotential eines Techniksystems ist die Kehrseite der Abhängigkeit einer Gesellschaft von dieser Technik.

Als Schaden soll ein unerwünschter Zustand gelten. Das Kriterium für dessen Unerwünschtheit ist aus der Perspektive des Bezugsobjekts zu wählen. Wenn nach der Verletzlichkeit der Gesellschaft gefragt wird, ist der Schaden aus der Perspektive der Allgemeinheit zu bestimmen. Hier können verfassungsrechtliche Zielbestimmungen als eine Orientierungshilfe dienen. Gilt das Interesse der Verletzlichkeit einer Organisation, ist deren Perspektive zu wählen, und wenn nach der Verletzlichkeit eines Individuums gefragt wird, ist diese Frage aus dessen Blickwinkel zu beantworten.

Die künftigen Anwendungen und ihre gesellschaftlichen Randbedingungen erlauben auch Aussagen zur **virtuellen Wahrscheinlichkeit** dieser Schäden. Sie setzt sich zusammen aus der Wahrscheinlichkeit unbeabsichtigten menschlichen und technischen 'Versagens' und der Wahrscheinlichkeit künftiger Motive sowie zukünftiger Aktionsmöglichkeiten bei heute üblichen Sicherungen.

Von großen Naturkatastrophen abgesehen, können alle unbeabsichtigt verursachten Schadensabläufe auch durch vorsätzliche Handlungen ausgelöst werden. Da vorsätzliches Handeln darüber hinaus weitere Schäden anrichten kann, führt es zu einem breiteren Schadensspektrum. Vorsätzliche Aktionen sind somit die 'Umhüllenden', die das Schadenspotential anderer Ursachen abdecken. Daher untersuchen Verletzlichkeitsanalysen vor allem den Mißbrauch von Techniksystemen. Unter Mißbrauch soll jeder Umgang mit einer Technik verstanden werden, der nicht ihrer gesellschaftlich akzeptierten Funktionsbestimmung entspricht. Er ist zu unterscheiden vom bestimmungsgemäßen Gebrauch der Technik, der in der Regel durch den jeweiligen Eigentümer oder Verfügungsberechtigten oder für die Allgemeinheit durch die zuständigen staatlichen Organe festgelegt wird. Der Gebrauch der Technik kann ebenfalls negative gesellschaftliche Folgen haben. Diese Folgen sind aber an anderen Kriterien zu messen - etwa dem der Verfassungsverträglichkeit (Roßnagel u.a. 1990b) - und mit anderen Maßnahmen zu verhindern oder zu bekämpfen. In der Verletzlichkeitsuntersuchung begrenzen wir uns daher auf die Untersuchung von Mißbrauchsmöglichkeiten und -folgen.

Virtuelles Schadensausmaß und virtuelle Wahrscheinlichkeit des Mißbrauchs determiniert die Notwendigkeit und den **Intensitätsgrad der künftigen Sicherungsmaßnahmen**. Diese werden bestimmt durch die künftigen technischen und organisatorischen Sicherungsmöglichkeiten und deren Grenzen. Das tatsächliche Sicherungsniveau hängt allerdings weniger von den Sicherungsmöglichkeiten als vielmehr von deren Realisierung und ihrer Verlässlichkeit ab. Es ist unter Berücksichtigung kontraproduktiver Effekte, Zielkonflikte, knapper Ressourcen und Widerstände sowie der organisatorischen, menschlichen, sozialen und politischen Voraussetzungen jedes Sicherungssystems abzuschätzen. Schließlich wirken auch die sozialen Kosten der Sicherheitsproduktion auf das Schadenspotential und das Sicherungsniveau zurück.
Als Ergebnis der Untersuchung sind qualitative Aussagen zur Verletzlichkeit einer vernetzten Gesellschaft möglich, die mit der gegenwärtigen Verletzlichkeit der Gesellschaft verglichen werden können. Diese Veränderungen der Verletzlichkeit unserer Gesellschaft sind allerdings nicht zwangsläufig. Ihre Analyse soll vielmehr zeigen, wo die Risiken und Folgen der Verletzlichkeit der Gesellschaft zu hoch sind, wo also Bedürfnisse und Ansatzpunkte für eine sozialverträgliche Gestaltung der Technik bestehen.
Die Verletzlichkeitsanalyse dient der Information aller Interessierten über mögliche gesellschaftliche Auswirkungen technischer Entwicklungen und Entscheidungen. Sie bewegt sich daher von Anfang an im Kontext politischer Bewertungen. Die Bedeutung, die einer Mißbrauchsmöglichkeit, einer Sicherungsmaßnahme, einer Schadensfolge oder einem Verletzlichkeitsaspekt zukommt, ist als eine Frage politischer Bewertung im demokratischen Willensbildungsprozeß zu bestimmen. Die Verletzlichkeitsanalyse kann letztlich nur versuchen, die untersuchte Technik, die Anwendungsfälle und die Mißbrauchs- und Schadensmöglichkeiten so auszuwählen, dass sie im Hinblick auf das Ziel der Untersuchung von der Mehrzahl der an der politischen Diskussion Beteiligten akzeptiert werden können: Ihre Darstellung soll eine Grundlage dafür sein, die Verletzlichkeit eines bestimmten Techniksystems zu bewerten und Schlußfolgerungen für die Technikgestaltung zu ziehen.

2. Frühere Erkenntnisse zur Telekommunikation

In der Literatur ist zwar eine wahre Flut von Veröffentlichungen zur technischen Sicherheit von Informations- und Kommunikationssystemen zu finden. Erstaunlicherweise befinden sich unter ihnen aber nur wenige Untersuchungen zur Verletzlichkeit, also zu den Ursachen und Folgen von Gefährdungen für die Gesellschaft. Von diesen befassen sich die meisten nur mit Teilfragen der Verletzlichkeit, wie zum Beispiel den „Hackern" und ihrer Motivation. Auch das Bundesamt für die Sicherheit in der Informationstechnik, zu dessen Aufgaben auch Technikfolgenabschätzung zählt, hat bisher nur zwei eingeschränkte Untersuchungen zu Chipkarten im Gesundheitswesen und zur Informationstechnik zur Fahrerunterstützung im Straßenverkehr durchgeführt (BSI 1995a und b). Auswirkungen auf die Gesellschaft als Ganze wurden bisher nur sehr selten untersucht.
Die früheste bekannte Studie ist die 1979 veröffentlichte Untersuchung des Schwedischen Verwundbarkeitskomitees (SARK 1979) „Datenverarbeitung und die Verwundbarkeit der Gesellschaft". In dieser wurden für Schweden Gefährdungen, etwa durch den Mißbrauch von Daten in öffentlichen Registern zusammengetragen. Sie war gegenwartsbezogen und enthielt kaum Bezüge zur Telekommunikation. Die erste Verletzlichkeitsuntersuchung für die Bundesrepublik „Die Verletzlichkeit der Informationsgesellschaft" wurde im Rahmen des Programms „Sozialverträgliche Technikgestaltung" des Landes Nordrhein-Westfalen 1988 von der „Projektgruppe verfassungsverträgliche Technikgestaltung" erstellt (Roßnagel u.a. 1990a). Seitdem wurde jedoch, abgesehen von einer US-amerikanischen Studie zur technischen Verwundbarkeit der Netze (NRC 1989) keine das Thema umfassend behandelnde Studie mehr veröffentlicht. Dies rechtfertigt es, einige auf die Telekommunikation bezogene Ergebnisse unserer Studie vorzustellen. Sie sollen im

folgenden Kapitel im Lichte neuerer Entwicklungen bewertet werden. Die Darstellung erfolgt thesenartig und konzentriert sich auf das damals im Vordergrund der Diskussion stehende Problem der „Verfügbarkeit".

Die Abhängigkeit vom Funktionieren der Telekommunikation nimmt stark zu

Anhand von Prognosen und Visionen von Entscheidungsträgern und Befürwortern einer weitgehenden Informatisierung der Gesellschaft wurden zunächst Szenarien der Entwicklung und Anwendung von Informations- und Kommunikationstechniken entworfen. Für die Telekommunikation zeigte sich dabei in den betrachteten gesellschaftlichen Bereichen durchweg ein Trend zur zunehmenden Anwendung von Telekommunikationsdiensten. Verallgemeinerungsfähig war insbesondere, dass die bis dahin noch überwiegend isolierten Anwendungen von Computern, seien es zentrale Rechenzentren in Betrieben oder Verwaltungen, seien es PCs an Arbeitsplätzen oder Homecomputer im Haushalt, künftig zunehmend vernetzt oder durch vernetzte Systeme ersetzt werden. Aufgrund dieser intendierten Entwicklung wurde eine hohe Abhängigkeit der Gesellschaft von Telekommunikation prognostiziert. Diese ergab sich einmal aus der Gleichzeitig- bzw. Gleichartigkeit der Entwicklung in den genannten Bereichen. Zum anderen wurde sie dadurch gefördert, dass bestehende Verfahren ersetzt oder verdrängt werden sollten, weil mit den Telekommunikationstechniken räumliche und zeitliche Schranken überwunden werden können, die mit den konventionellen Mitteln nicht zu überwinden sind.

Störungen der Telekommunikation können durch die Schadensdynamik zu Katastrophen führen.

In der Analyse möglicher Gefährdungen der Telekommunikation und ihrer Folgen zeigte sich, dass Schäden bei Informations- und Kommunikationssystemen einige für sie typische Schadensverläufe aufweisen, die ihre besondere Problematik auch im Vergleich zu anderen Techniksystemen und herkömmlichen Informations- und Kommunikationsmitteln begründen:

- Schäden können „multipliziert" werden, wenn fehlerhafte oder manipulierte Systeme in verschiedenen Bereichen verwendet werden oder wenn Netze zu ihrer Verbreitung genutzt werden (Multiplikationsschäden),
- Schäden können vervielfacht werden, weil Schwachstellen der eingesetzten Systeme zu vielfachen voneinander unabhängigen Handlungen verleiten (Kumulationsschäden).
- Schäden können besonders hoch werden (hoher Einzelschaden), weil die neuen technischen Möglichkeiten bisherige Grenzen von Raum, Zeit, Energie oder Informationsdichte zu durchbrechen vermögen.
- Schäden in Netzknoten und anderen Komponenten vernetzter Systeme können sich in verschiedenen Systemen und den darauf aufbauenden Anwendungssystemen auswirken und die Schäden vervielfachen (Komplexschäden).
- Schäden können trotz räumlich und zeitlich vollständiger Entkopplung trotzdem gleichzeitig auftreten, wenn sie dieselben Programme nutzen oder mit denselben manipulierten Werkzeugen entwickelt wurden, eine bei anderen Techniksystemen unbekannte Gefährdung besonderer Tragweite (Kopplungsschäden).

Durch Softwaremanipulation könnten Systemschäden verursacht werden, durch die die Telekommunikation großflächig ausfallen könnte. Entsprechend der damaligen Vision des Glasfaser-Universalnetzes für alle Haushalte und Betriebe wäre dann nahezu die gesamte Telekommunikationsinfrastruktur ausgefallen. Neben den unmittelbaren Folgen für die auf Telekommunikation angewiesenen Betriebe, Verwaltungen und Privatpersonen träten in der Folge eine Reihe weiterer Schäden auf, die sich wechselseitig verstärken würden. Katastrophale Schadensprozesse, die die Fähigkeit der Gesellschaft übersteigen, sie zu bewältigen, konnten nicht ausgeschlossen werden (Roßnagel/Pordesch 1989).

Zahl und Varianten von Mißbrauchsmotiven nehmen zu

Die Auswertung von mehr als 1000 Mißbrauchsfällen und die Übertragung der Ergebnisse auf die prognostizierten technischen und gesellschaftlichen Entwicklungen ließ ein breit gestreutes Feld von Motiven für Angriffe auf Informations- und Kommunikationssysteme erwarten.

Für die weitere Entwicklung wurde angenommen, dass keines der bisherigen Motive entfallen würde. Typische persönliche Motive waren der Ärger über Entlassungen, Streß und Neugier. Bereicherungsmotive waren nahezu überall dort zu finden, wo mit Informationen geldwerte Verfügungen erfolgen. Viele Mißbrauchsaktionen waren auch politisch motiviert, von Abhöraktionen bis hin zu Brand- und Bombenanschlägen. Zu diesen wurden aus den spezifischen Bedingungen der künftigen Informationsgesellschaft weitere Mißbrauchsmotive abgeleitet. Gedacht wurde hier insbesondere an von Arbeitsverdichtung, Dequalifizierung, Arbeitsplatzverlust und sozialem Abstieg Bedrohte und Betroffene, die Informations- und Kommunikationstechnik für diese Folgen verantwortlich machen und angreifen könnten. Eine Zunahme krimineller Motive wurde wegen des steigenden Wertes von Informationen erwartet, welcher zusätzliche Anreize für Bestechung, Spionage, Erpressung und Manipulationen geben würde. Durch den zunehmend vernetzten elektronischen Geld- und Warenverkehr wäre mit neuen Formen der organisierten Computerkriminalität zu rechnen. Neue politische Motive wurden durch die zunehmende Wirtschaftsspionage im Zuge der internationalen Konkurrenz und durch internationalen Terrorismus erwartet. Schließlich wurde angenommen, dass neue Formen sozialen Widerstands mit Hilfe der neuen Technologien ausgetragen würden - von Blockaden elektronischer Zufahrtswege bis hin zur gezielten Überlastung von Telekommunikationsdiensten. Insgesamt wurde mit einem im Vergleich zum fortschreitenden Technikeinsatz überdurchschnittlich zunehmenden Anreiz für Mißbrauchsaktionen gerechnet.

Trotz vorhandener Redundanzen sind die Netze verwundbar

Um das Bild der künftigen Bedrohungslage im Sinn der Sicherheitsverantwortlichen zu konstruieren. wurden die aus der Fallsammlung ausgewerteten Angriffsmöglichkeiten auf die prognostizierten Nutzungsformen übertragen. Dabei zeigte sich, dass von Insidern die größten Gefährdungen ausgehen. Insbesondere Programmierer, Systemverwalter und Wartungstechniker haben vielfältige Möglichkeiten, unbemerkt Manipulationen durchzuführen. Dieser Personenkreis hat die Gelegenheit und das Know-how, Programme zu manipulieren oder manipulierte Programme einzuspielen. Sie können so unbemerkt Zugangsmöglichkeiten eröffnen („Falltüren"), Systemmanipulationen durchführen („trojanische Pferde") und zu bestimmten Zeitpunkten Systeme zum Absturz bringen („logische Bomben"). Die Digitalisierung der Vermittlungstechnik würde im Falle einer geeigneten Insidermanipulation zu besonders großen Schäden führen, weil durch einen gezielten Schlag ein Großteil der Knoten des integrierten Telekommunikationsnetzes ausfallen könnte. (Pordesch 1989).

Gegenüber externen Angreifern weist das Übertragungsnetz einen erheblichen Grundschutz auf, weil die Fernmeldenetze auf der überörtlichen Ebene redundant und vermascht sind (Zwei-Wege- und Zwei-Medienführung). Dennoch treten an vielen Stellen räumliche Konzentrationen von logisch gesehen dezentralisierten Netzfunktionen auf, bei denen gezielte Einzelaktionen mit Gewaltanwendung Schäden großer Wirkungsbreite entfalten können. Außerdem zeigten einige Fälle, dass auch ein in der Fläche ausgedehntes System durch koordiniert vorgebrachte Aktionen schwer geschädigt werden kann. Schließlich können auch Externe die Netze für die rasche Verbreitung manipulierter Programme nutzen (Viren) oder die Netze damit überlasten (Würmer)

Das Sicherungsniveau ist potentiell hoch, tatsächlich aber begrenzt

Für alle Anwendungsbereiche konnten sehr weitgehende Sicherungsmöglichkeiten und somit ein sehr hohes theoretisches Sicherheitsniveau aufgezeigt werden. In den Telekommunikationsnetzen ist bereits ein gewisses Maß an Redundanz eingebaut, das die Schäden isolierter Angriffe begrenzt.

Logische Zugangssicherungen, Softwarequalitätssicherung und andere Maßnahmen wurden eingesetzt, Verschlüsselungsmöglichkeiten zum Schutz der Nachrichtenübertragung zeichneten sich ab.
Gegenüber Insidern können jedoch viele dieser Maßnahmen nur begrenzte Wirksamkeit entfalten. Es wurde erwartet, dass das tatsächliche Sicherungsniveau durch die Erfordernisse des reibungslosen Betriebs und durch kontraproduktive Effekte von Sicherungsmaßnahmen begrenzt würde. Ein Beispiel hierfür war etwa der Konflikt zwischen dem Schutz der Vertraulichkeit durch Verschlüsselung einerseits und dem Risiko des Datenverlustes bei Verlust des Schlüssels andererseits. Neben diesen technischen Gründen wurden durch begrenzte Etats „menschliche Schwächen", soziale Hemmnisse und Organisationsprobleme Lücken im Sicherungssystem und dessen Umsetzung erwartet.
Zusammenfassend wurde prognostiziert, dass die Telekommunikation zu einem elementaren Versorgungssystem der Informationsgesellschaft wird, dessen Bedeutung und Gefährdung dem der Stromversorgung entsprechen würde. Der Netzbetreiber - zum Zeitpunkt der Untersuchung ausschließlich die „Deutsche Bundespost" - garantierte ein hohes Maß an Grundsicherung. Dies wäre allerdings außergewöhnlichen Herausforderungen, wie Krieg, Terror oder massiven Insiderangriffen nicht gewachsen. Als Gegenmaßnahmen wurden zusätzliche präventive Sicherungsmaßnahmen, wie vermehrte Redundanzen und Diversifizierungen, vorgeschlagen. Daneben wurde aber betont, dass es auch darum gehen müsse, die Abhängigkeit von der Telekommunikation zu reduzieren, indem auf Seiten der Anwender und Nutzer Alternativen geschaffen, Pufferungsmöglichkeiten vorgehalten und nichttechnische Ersatzsysteme erhalten werden. Bei der Durchsetzung dieser Forderungen wurde neben der Bewußtseinsbildung durch kritische Diskurse explizit auf staatliche Regulierungsmaßnahmen durch Gesetzgebung, Zulassungsverfahren und Haftungsrecht gesetzt.

3. Aktuelle Entwicklungstendenzen

Seit diesen Untersuchungen Ende der 80er Jahre haben sich sowohl die Telekommunikationspolitik als auch die gesellschaftlichen Rahmenbedingungen wesentlich verändert. Eine neue Untersuchung zur Verletzlichkeit würde demzufolge andere Entwicklungspfade prognostizieren und andere Schwerpunkte setzen. Diese notwendige neuerliche Untersuchung wurde bisher nicht geleistet. Im folgenden können jedoch die bisherigen Ergebnisse mit neueren Entwicklungstrends kontrastiert werden, um so Eingangshypothesen für künftige Untersuchungen zu gewinnen.

3.1 Wichtige Änderungen der letzten 10 Jahre

Mittlerweile wurde eine umfassende **Deregulierung**, Liberalisierung und Privatisierung der Telekommunikation durchgeführt. Ein Ergebnis des 1998 voll einsetzenden Wettbewerbs dürfte unter anderem sein, dass es mehrere Anschluß- und Verbindungsnetze unterschiedlicher privater Betreiber gibt und definitiv kein Universalnetz einheitlicher Technik eines staatlichen Betreibers.
Die Vorstellungen einer Versorgung aller Haushalte und Betriebe mit breitbandiger Individualkommunikation per Glasfaser hat sich vor allem wegen der Kosten und der mangelnden Nachfrage als zu optimistisch herausgestellt und einer **wirtschaftlichen Ernüchterung** Platz gemacht. Die Visionen der Technikprotagonisten richten sich derzeit auf das „organisch wachsende", internationale Netz, für die das Internet zugleich Hintergrund und Metapher darstellt.
Die kritische Öffentlichkeit Ende der 80er Jahre ließ erwarten, dass auch künftig die Telekommunikationspolitik zum Kristallisationspunkt öffentlicher Auseinandersetzungen werden könnte. Heute wird die öffentliche Diskussion neben kritischen Äußerungen vor allem durch einen Wettlauf um die Aneignung der neuen Techniken geprägt. Die Anzeichen für eine Projezierung von Ängsten vor Arbeitsplatzverlust und wirtschaftlichem Abstieg auf die Technik sind **zunehmender**

Akzeptanz gewichen. Insbesondere bei der Neubewertung möglicher Motive im Sinne der für Sicherheit Verantwortlichen wäre dies zu berücksichtigen.

3.2 Mögliche Auswirkungen auf die Verletzlichkeit

Schäden geringerer Wirkungsbreite

Welche „Mitspieler" sich auf dem vollständig liberalisierten Telekommunikationsmarkt ab 1998 gegen die Telekom durchsetzen können, ist noch nicht abzusehen. Wahrscheinlich ist allerdings, dass auch bei leitungsgebundenen Netzen und im klassischen Telefondienst mehrere Wettbewerber auftreten werden, zu denen Konsortien unter Beteiligung der Elektrizitätsversorgungsunternehmen und der Bundesbahn gehören werden. Die neuen Anbieter werden vor allem Weitverkehrsnetze betreiben, bei denen Verbindungen über die vorhandenen Trassen oder Satelliten ausgebaut werden können. Im Teilnehmeranschlußbereich sind zusätzliche Kabelnetze wegen der hohen Kosten selten rentabel. Hier ist jedoch zu erwarten, dass private Anbieter mit kleinräumigen Mobilfunknetzen zumindest in einigen städtischen Bereichen eine Infrastruktur auch im Teilnehmeranschlußbereich aufbauen werden. Gleichzeitig kann der ohnehin bereits boomende Mobilfunkbereich mit satellitengestützten Mobilfunkempfängern einen weiteren Aufschwung erhalten.

Wo welche Systeme aufgebaut werden und welche Struktur die neuen Netze insgesamt erhalten werden, ist kaum vorherzusagen. Mögliche Optionen und Szenarien haben jedoch in jedem Fall davon auszugehen, dass die Telekommunikationsinfrastruktur vielfältiger wird, als dies heute der Fall ist. Dies gilt sowohl für die eingesetzten Techniken der Endgeräte, Vermittlungs- und Übertragungssysteme als auch für deren organisatorischen Aufbau. Zu vermuten ist, dass die entstehende Vielfalt die Wirkungsbreite isolierter logischer und physischer Angriffe auf die Verfügbarkeit gegenüber homogenen Universalnetzoptionen reduziert. Denn ein isolierter Angriff beträfe nur einzelne Netze oder Hard- und Softwaresysteme, wohingegen andere Systeme weiterhin funktionieren dürften. Nachteilig im Hinblick auf Systemgefährdungen könnte es sich auswirken, wenn viele Betreiber einheitliche Systeme verwenden und wenn die Konkurrenz zu einer erheblichen Verringerung der Redundanzen und anderer Sicherheitsvorkehrungen führen würde. Wesentlich wird auch sein, wo und wie die intelligenten Netzfunktionen realisiert werden. Beziehen die Anwender sämtliche für ihre Systeme notwendigen Programme und Daten aus dem Netz und werden auf die Telekommunikation bezogene Dienstleistungen, wie künftige Formen der Nachrichtenspeicherung und Umleitungen so realisiert, wie sich das Enthusiasten des „Netzwerk-PCs" vorstellen, könnten die technische Abhängigkeit von Telekommunikationsnetzen und die Risiken von Manipulation und Ausforschung steigen. Geringer könnten diese Risiken jedoch sein, wenn solche „höheren Funktionen" (Intellienz) in die Endgeräte verlagert und unter die Kontrolle der Teilnehmer gestellt werden. Vielleicht ließen sich diese Entwicklungsmöglichkeiten zu zwei Entwicklungspfaden der Informationsgesellschaft bündeln - einem „ Pfad der Netzdienstleistungen" und einem „Pfad benutzerkontrollierter Endgeräte". Ob diese idealtypischen Gedankenkonstruktionen Problemlagen verdeutlichen oder eine gesellschaftliche Verzweigungssituation beschreiben, hängt von den Einwirkungsmöglichkeiten auf die Entwicklung ab, die nach der Liberalisierung neu identifiziert werden müssen.

Für Verletzlichkeitsuntersuchungen wären Schwerpunktverlagerungen vorzunehmen: Während die Gefährdungen der Verfügbarkeit der Netze und die damit verbundene Verletzlichkeit mit den genannten Einschränkungen abnehmen kann, werden andere Risiken zunehmend bedeutsam, die bisher nicht derart im Vordergrund standen. Relevant erscheinen hier u.a. folgende Entwicklungstrends:

Die Privatisierung verringert die Transparenz des Netzgeschehens und staatliche Steuerungsmöglichkeiten

Vor den Postreformen war die Telekommunikation mit wenigen Ausnahmen in der Hand eines Betreibers und unter der Kontrolle eines Ministeriums. Staatliche Interessen an der Verfügbarkeit der Telekommunikation in Verteidigungs- und Katastrophenfällen und der Bevorzugung staatlicher Instanzen in solchen Fällen, der Erhaltung des Datenschutzes und eines Sicherheitsstandards konnten vermittels einer Ministerialbürokratie und deren Durchgriff auf Postdirektionen und fernmeldetechnische Ämter sehr direkt geltend gemacht werden. Auch wenn diese Sicherheitsinteressen nicht deckungsgleich mit denen von Firmen, Bürgern und der „Allgemeinheit" waren, garantierte das bisherige System ein erhebliches Maß an Grundsicherheit und Steuerungsmöglichkeiten. Sobald viele Netz- und Dienstbetreiber sich den Markt der Telekommunikation aufteilen, wird sich diese Situation ändern. Ein im scharfen Wettbewerb stehender Betreiber kann es sich kaum erlauben, Vermittlungsstellen, Übertragungsstrecken und Ersatzanlagen nur für unwahrscheinliche Krisenfälle aufrechtzuerhalten. Er wird kaum geneigt sein, technische Sicherungsmaßnahmen, wie Vorrangschaltungen, Gebäudesicherungen oder Mitarbeiterschulungen, die seinen Kunden kaum erkennbaren Nutzen bringen, zu finanzieren. Daneben dürfte die Privatisierung auch zu faktischen Problemen führen, Risiken richtig zu erkennen und adäquate Maßnahmen zu bestimmen. Im schärfer werdenden Wettbewerb werden Telekommunikationsverbindungen in einem komplexen leitungsgebundenen, mobilfunk- oder satellitengestützten Netzwerk höchst unterschiedlicher Dienstleistungs- und Netzanbieter so geschaltet, dass die kurzfristigen Kosten minimiert werden. Eine Verbindung zwischen zwei Städten - kostengünstig bei einem über das Netz der Telekom angewählten Dienstleistungsverkäufer angemietet - mag über das Weitverkehrsnetz eines Stromversorgers und Außenstrecken eines Corporate Networks einer Firma gehen. Im ungünstigen Fall landet der Rufer über den Anrufweiterleitungsdienst des intelligenten Netzes bei einem Telekommunikationsbürodienst, der ihm mitteilt, dass der Gerufene nicht erreichbar ist. Es dürfte schon schwierig sein, solche Ketten nachzuvollziehen. Noch schwieriger ist es, die Schadensrisiken und Sicherungsanforderungen solch komplexer Netzwerke in Relation zur Abhängigkeit der Gesellschaft von ihnen und zu den möglichen Schäden eines Störfalls zu bestimmen.

Die Globalisierung vergrößert Mißbrauchsmöglichkeiten, -motive und -schäden

Durch die Verbreitung der Online-Dienste und ihrer technischen Infrastrukturen, inbesondere des Internet, entsteht derzeit rascher als früher angenommen, eine globale Telekommunikationsinfrastruktur. Erfolgt die Kommunikation international, entschwindet sie jedoch dem nationalen Einflußbereich. Gewaltverherrlichung, Pornographie, unlauterem Wettbewerb, Urheberrechts- und Ehrverletzungen kann der Staat nicht wirkungsvoll entgegentreten. Falschinformationen können von irgendwoher verbreitet werden, Angriffe auf Anwender können von jedem Winkel der Erde aus gestartet werden, ohne dass ein Betreiber oder Staat dies verhindern und oder auch nur den Verursacher erkennen und zur Rechenschaft ziehen kann. Die Wahrscheinlichkeit, bei strafbaren Handlungen in den globalen Netzen nicht erkannt und erst recht nicht haftbar gemacht werden zu können, erhöht die Motivation für Mißbrauchsversuche und damit deren Wahrscheinlichkeit. Die Globalisierung vergrößert jedoch auch das Ausmaß möglicher Schäden. Informationen über verfügbare Gewaltdarstellungen und Pornographie verbreiten sich ebenso rasch wie gefährliche Viren oder „Würmer" und Informationen über Schwachstellen genutzter Programme.

Der Staat kann mittels seiner Strafverfolgungsbehörden nur dort eingreifen, wo die immaterielle Welt des Netzes auf seinem Territorium in die körperliche Welt von Netzzugangspunkten, Servern und Anwendern übergeht. Er kann nur dann Täter festnehmen, Geräte und Datenträger beschlagnahmen, wenn diese sich auf seinem Territorium aufhalten. In der körperlosen Netzwelt jedoch ist er machtlos (Roßnagel 1997).

Für die Sicherheit in der Telekommunikation werden Selbstschutzstrategien an Bedeutung gewinnen

Zunehmende Ohnmachtserfahrungen des Staates werden weitere Folgen nach sich ziehen. Kann der Staat nicht ausreichend für den Schutz der Bürger in der immateriellen Welt sorgen, werden die Nutzer versuchen (müssen), sich selbst zu schützen. Ansätze für solche Selbstschutzstrategien sind heute schon zu beobachten: Programme für Verschlüsselung und Steganographie werden verbreitet, mit denen jeder die Vertraulichkeit seiner gespeicherten und übermittelten Nachrichten sichern kann. Mit Erreichbarkeitsmanagementsystemen kann jeder seine telekommunikative Erreichbarkeit durch Filter und technikgestützte Aushandlungsprozesse regeln und beabsichtigte oder unbeabsichtigte Störungen reduzieren. Durch Anmieten von Zugängen bei unterschiedlichen Betreibern und Nutzung der Angebote unterschiedlicher Anbieter kann der Einzelne seine Abhängigkeit gegenüber Firmen und Institutionen verringern. Mit neuen Filterprogrammen können Teilnehmer selbst festlegen, auf welche Fernsehsendungen und Informationen im Netz ihre Kinder zugreifen können. Mit digitalen Signaturen können sie die Integrität ihrer Nachrichten schützen und mit Pseudonymen ihre informationelle Selbstbestimmung sichern.

Neben den positiven Wirkungen eines Benutzerselbstschutzes im Sinne von Selbstbestimmung und Selbstverantwortung sind jedoch auch problematische Formen des Selbstschutzes zu erwarten. Wo etwa gegenüber der Verbreitung von Gewaltdarstellungen oder Pornographie oder dem Mißbrauch von Daten kein wirkungsvoller Selbstschutz möglich ist, könnten sich auch aktive Formen der Gegenwehr im Sinne einer „elektronischen Bürgerwehr" oder „elektronischen Selbstjustiz" entwickeln. Solche Möglichkeiten reichen von Boykottstrategien, die über das Netz besonders leicht und rasch zu verbreiteten sind, bis hin zu Blockaden elektronischer Zufahrtswege, Informationsüberflutung, elektronischen Einbrüchen und gezielter Desinformation.

Eine neue zukunftsorientierte Untersuchung der Verletzlichkeit der Telekommunikation steht noch aus. Vieles scheint darauf hinzudeuten, dass die Risiken für die Verfügbarkeit geringer werden, während Gefährdungen in Bezug auf die Inhalte der Telekommunikation zunehmen. Entsprechend dieser veränderten Risikolage und den reduzierten staatlichen Einflußmöglichkeiten sind auch veränderte politische Strategien notwendig.

Sicher bleibt die Gestaltung der informationstechnischen Infrastrukturen durch rechtliche Regulierung wichtig. Solche Regulierungsmaßnahmen sollten auf die Sicherstellung der Telekommunikationsversorgung, Datensparsamkeit und auf technische und organisatorische Maßnahmen zum Datenschutz zielen. Daneben ist es jedoch eine politische Aufgabe, teilnehmerkontrollierten Selbstschutz zu fördern. Manche dieser Mittel - zum Beispiel das Verschlüsselungsprogramm PGP - können ohne jede Vorleistung genutzt werden. Hier muss der Staat nur auf hinderliche Regelungen verzichten. Andere Maßnahmen - wie digitale Signaturen - sind auf eine Infrastruktur angewiesen, die es dem Einzelnen ermöglicht, die Selbstschutzinstrumente zu nutzen (Roßnagel 1996; Hammer 1995).

4. Verletzlichkeit einer durch das Internet vernetzten Gesellschaft

Die ausstehende Verletzlichkeitsuntersuchung wird im abschließenden Teil am Beispiel des Internet genauer konturiert.

4.1 Modellfall Internet?

Die Entwicklung des Internet ist für die Verletzlichkeit der Gesellschaft von erheblicher Bedeutung. Zum einen hat das Internet mit seinen Diensten, insbesondere WWW und E-Mail, aufgrund der enormen Zuwachsraten von monatlich mehr als 10 % und schon ca. 50 Millionen Teilnehmern weltweit eine erstaunliche Erfolgsgeschichte. Es entwickelt sich zum wichtigsten Netzwerk für

kommerzielle Online-Dienste. Es bildet bildet bereits die infrastrukturelle Grundlage offener Telekooperation und eines internationalen elektronischen Marktplatzes. Zum anderen ist die Entwicklung des Internet in mehrerlei Hinsicht typisch für die veränderte Formen der Entwicklung der Telekommunikationsnetze und -dienste insgesamt:

- **Hohe Entwicklungsdynamik:** Dienstleistungen und Angebote im Internet befinden sich in einem raschen Wandel. Viele neue Dienstleistungsangebote und Nutzungsformen, die hier von zunächst wenigen Teilnehmern und Anbietern ausprobiert werden, können später auch in anderen Telekommunikationsnetzen Bedeutung erhalten. Rechtlich problematische, sicherheits- und datenschutzkritische Nutzungsformen, Motive und Möglichkeiten von Angreifern, die bei breiterer Nutzung künftig zu gravierenden Schäden führen könnten, können hier im Ansatz bereits beobachtet werden.
- **Internationalisierung:** Das Internet ist das bei weitem wichtigste, weltweit genutzte offene Telekommunikationssystem. Die Internationalisierung der Informationsströme und die daraus resultierenden Probleme internationaler Abhängigkeiten lassen sich am Internet besonders gut untersuchen.
- **Kommerzialisierung und rechtsverbindliche Kooperation.** Mit dem WWW ist innerhalb kurzer Zeit ein einfach zu bedienender Informationsdienst entstanden, der sich auch im Hinblick auf kommerzielle Anwendungen rasch entwickelt. Die Nutzung von Zahlungssystemen im Internet, die gerade erst begonnen hat, dürfte diese Entwicklung erheblich beschleunigen. Gleichzeitig wird das Internet zur bedeutendsten Infrastruktur für den Austausch elektronischer Post. Immer mehr Transaktionen über das Internet haben rechtsverbindlichen Charakter. Sicherheitsschwachstellen und Regelungsdefizite, bisher aufgrund der geringen Verbreitung rechtsverbindlicher Kooperation nur virulent, könnten rasch zu erheblichen Sicherheits- und Akzeptanzproblemen führen.
- **Dezentrale und private Organisationsform:** Das Internet und Internet-Dienste werden anders als konventionelle Telekommunikationsnetze und -dienste nicht von einer staatlichen Institution geplant. Von verschiedenen Gremien werden Standards entwickelt, deren Etablierung Sache des Marktes ist. Das Internet ist kein einheitliches Netz in Besitz einer Telefongesellschaft, sondern besteht aus sehr vielen privaten Netzen und Vermittlungssystemen im Besitz von Universitäten, Institutionen und Firmen. Internet-Dienste werden von vielen Betreibern zu unterschiedlichen Konditionen und mit unterschiedlichen Leistungen angeboten. Das Netz und seine Angebotsstruktur entwickeln sich im direkten Wechselspiel zwischen Angebot und Nachfrage. Bisher hat diese Form der Selbstregulierung nicht zu großen Instabilitäten des Netzes geführt. Die Form des Netzes hat sogar große Vorteile für eine Begrenzung des Schadenspotentials. Eine andere Frage ist jedoch, inwieweit die daraus wachsenden Netzstrukturen, Dienstleistungsangebote und Nutzungsformen auch möglicherweise stark veränderten Sicherheitsanforderungen der Zukunft genügen.
- **Individueller Selbstschutz statt Systemschutz:** Das Internet und seine Dienste bieten wenig Grundsicherung. Es gibt keine einheitlichen Verfahren gegen Einbrüche, Lauschaktionen und Störungen, gegen Verirrungen im Netz, Informationsüberflutung und Täuschungen. Der Grad an erreichbarer Sicherheit hängt deshalb im wesentlichen von den Schutzmaßnahmen der Anwender und lokalen Anbieter ab. Daneben etablieren sich Verschlüsselungs- und Signaturverfahren ohne eine geplante, vereinheitlichte Sicherungsinfrastruktur. Die Frage ist jedoch, ob diese Formen des Selbstschutzes unter Marktbedingungen zu einem ausreichenden Sicherungsniveau führen und ob sich aus ihrem Zusammenwirken nicht neue Risiken ergeben können (Roßnagel 1996).

Am Internet können künftige Gefährdungen der Telekommunikation erkannt und geeignete sichernde Gestaltungsmaßnahmen und -strategien entwickelt werden. Dabei darf die Sicherheitsbetrachtung allerdings nicht wie bei den herkömmlichen Sicherheitsuntersuchungen auf technische Schwachstellenanalysen begrenzt werden. Die Anzahl der Möglichkeiten, das

Funktionieren des Netzes zu stören, ist zu groß und zu vielfältig, eine vorbeugende Berücksichtigung aller möglichen Gefährdungen daher praktisch unmöglich. Außerdem kann das, was heute im Rahmen einer ordnungsgemäßen Nutzung der Telekommunikation tolerierbar ist, unter veränderten Anwendungsbedingungen, neuen Motiven und Angriffsformen zu einem die Sicherheit gefährdenden Mißbrauch werden. Daher muss die technische Sicherheitsbetrachtung um eine soziale erweitert werden, der das Kriterium Verletzlichkeit mit der oben skizzierten Untersuchungsmethode Rechnung trägt. Im folgenden werden einige wesentliche Fragestellungen und Eingangshypothesen für eine Verletzlichkeitsuntersuchung am Beispiel des Internet aufgeworfen.

4.2 Entwicklungsoptionen des Internet und seiner Nutzung

Die technische Verwundbarkeit des Internet ist zwar nicht identisch mit dessen Verletzlichkeit, jedoch ein wesentlicher Faktor. Voraussetzung für die Abschätzung der Verwundbarkeit ist eine Analyse der teils bisher nur denkbaren Zukünfte des Internet. Sie entwickeln sich auf folgenden drei Ebenen:

Netzebene

Entscheidend für die technische Verwundbarkeit des Internet sind die Entwicklungen der Netzarchitektur und der künftigen Betriebsformen. Heute ist das Internet ein von privaten und öffentlichen Institutionen betriebenes Netzwerk von Vermittlungssystemen, dessen Rückgrat insbesondere Netzverbindungen der Hochschulen bilden. Die Verfügbarkeit dieses Netzes resultiert aus der Leistungsfähigkeit dieser Verbindungen und der paketorientierten Vermittlungstechnik des Internet, die speziell im Hinblick auf die Ausfallsicherheit konzipiert wurden. Ob das vorhandene Sicherheitsniveau künftigen Anforderungen gerecht werden wird, ist abhängig von der Weiterentwicklung des Netzes und seiner Nutzung. Zunehmend orientiert sich die Netzentwicklung an Marktgesichtspunkten, wobei auftretende Verkehrsengpässe und andere Schwierigkeiten Anlässe für Maßnahmen der Beteiligten bilden. Wie verwundbar das Netz in technischer Hinsicht ist, wäre durch eine Untersuchung des Netzaufbaus und seiner Entwicklung zu klären. Dabei ist zu berücksichtigen, dass sich das Internet auf unterschiedlich sichere öffentliche und private Übertragungsnetze abstützt und auf technischer Ebene (bei den Servern und Endsystemen) aus Systemen weniger Hersteller besteht. Dadurch dürfte das Netz gegenüber bestimmten Manipulationen und physischen Attacken verwundbarer sein, als aufgrund des Vermittlungsprinzips gemeinhin angenommen wird. Außerdem ist zu vermuten, dass entsprechend einer am kurzfristigen Bedarf orientierten Entwicklungslogik viele Fehler oder Manipulationen, die zwar möglich, bisher aber nicht aufgetreten sind, nicht berücksichtigt wurden und ohne besondere steuernde Maßnahmen auch weiterhin nicht berücksichtigt werden.

Dienste

Die heute im Internet angebotenen Basisdienste wie E-Mail und File-Transfer sowie neue Dienste wie das World Wide Web (WWW) weisen Schwachstellen auf, die bereits für Angriffe genutzt wurden. Solche liegen beispielsweise in der Fälschung von E-Mail-Adressen, der Überlastung von Servern durch Adreßfälschungen, im unbefugten Zugang zu angeschlossenen Rechnern und in der Möglichkeit für Betreiber, auf zu übertragende Daten zuzugreifen. Hierzu gibt es bereits zahlreiche Publikationen. Neue Untersuchungen hätten sich den Fragen zuzuwenden, wie sich die Dienste weiterentwickeln und welche neuartigen Probleme daraus resultieren könnten. Aktuelle Entwicklungen sind die Programmiersprache Java und Telefonverbindungen. In Zukunft sind

Bewegtbildübertragung und Erweiterungen in Richtung Virtual Reality zu erwarten. Neben der Entwicklung spezieller Diensteangebote sind die Zahlungssysteme im Internet von großer Bedeutung für die Verletzlichkeit, weil Angriffe auf die dazu notwendige Infrastruktur große Schäden verursachen können.

Nutzungsformen

Für den Nutzer werden die Zugangsmöglichkeiten zum Internet vereinfacht und verbilligt werden. Zugangsmöglichkeiten zu Internet-Diensten über Kabelfernsehnetze mit Rückkanal oder sogar über Mobilfunk und Personal Digital Assistants sind bald zu erwarten. Mit diesen Möglichkeiten könnte das Internet zu einem von breiten Bevölkerungskreisen genutzten Medium werden. Anders als heute, wo das Internet hauptsächlich noch für wissenschaftliche Zwecke und als Freizeitspaß für Computerbegeisterte genutzt wird, den Alltag der meisten Menschen jedoch kaum beeinflußt, könnte die Entwicklung künftig zu einer erheblichen Abhängigkeit der Gesellschaft vom Internet führen. Zugleich dürften viele Formen kriminellen Handelns auf dieses Medium übertragen werden. Dies wird neue Schutz- und Vorbeugemechanismen, Nachweis- und Überführungsmethoden erfordern. Von großer Bedeutung wird sein, wie sich sicherheitsrelevante Einstellungen und Verhaltenweisen verändern.
Die Handhabung der Internet-Dienste wird bereits heute durch spezifische Angebote wie Navigationshilfen unterstützt. Sie könnten künftig durch neue Konzepte ergänzt werden. Agenten etwa könnten den Benutzer bei Routineaufgaben unterstützen und ihm bei der Lösung komplexer Aufgaben im Netz helfen. Die neuen Hilfsmittel werden auch neue Gefährdungen verursachen - etwa die Ausforschung von Benutzerpräferenzen oder -verhalten durch Manipulation von Agenten.

4.3 Verletzlichkeitsaspekte

Mißbrauchsmotive und -möglichkeiten

In der Vergangenheit erfolgte Mißbrauch des Internet vornehmlich durch Hacker, die es benutzten, um in angeschlossene Rechnersysteme einzudringen. Mit der Verbreitung des WWW-Dienstes ist heute vor allem die strafbare Verbreitung bestimmter Informationen ins öffentliche Bewußtsein gerückt. Mit der zunehmenden Nutzung des Internet für geschäftliche Zwecke und den technischen Weiterentwicklungen könnten neue Möglichkeiten hinzukommen (Mann 1994), wie beispielsweise

- Angriffe auf Zahlungssysteme, Sicherungstechniken und Sicherungsinfrastrukturen für Verschlüsselung und Signaturen,
- Manipulation und Ausforschung neuer Hilfsmittel wie Intelligent Agents,
- Störung, Zerstörung oder gezielte Überlastung von Systemen der Internet-Provider,
- Angriffe auf die Netzinfrastrukturen und deren Unterstützungssysteme (etwa die Stromversorgung),
- Nutzung neuer Telekommunikationsdienstleistungen für betrügerische Angebote, das Etablieren von Phantomfirmen oder die Verbreitung von Falschinformationen.

Wie wahrscheinlich Angriffe sein werden, hängt u.a. von den möglichen Motiven von Angreifern ab. Motive für Angriffe durch Hacker waren in der Vergangenheit Spaß, der Wunsch nach Bestätigung oder das Ausspähen von Staats- oder Geschäftsgeheimnissen. Für andere Täter war die Möglichkeit, Informationen strafbaren Inhalts ohne Risiko der Strafverfolgung verbreiten zu können, entscheidendes Motiv. Zusätzliche Motive können beispielsweise folgen aus

- der wirtschaftlichen und gesellschaftlichen Bedeutung des Internet (Erpressung, Sabotage),

der zunehmenden internationalen Wirtschaftsspionage oder

der Abwehr politisch umstrittener Formen der Netzüberwachung, Zensur und Kontrolle

Abhängigkeit und Schadensmöglichkeiten

Die Größe möglicher Schäden hängt davon ab, welche gesellschaftlichen Funktionen auf das Internet übertragen werden und wie wirksam mögliche schadensreduzierende Mechanismen in betroffenen sozialen Systemen sind. Die breite Nutzung des Internet zur unternehmensinternen und zur offenen Telekooperation wird viele bisher genutzte Telekommunikationsformen ersetzen. Daneben könnten auch traditionelle bisher von konventionellen Medien erbrachte Kooperationsformen substituiert werden. Vorhandene Infrastrukturen, wie die Briefpost oder traditionelle Zahlungssysteme, werden dadurch möglicherweise abgebaut. Gleichzeitig könnten sich mit der verstärkten Nutzung von Internetdienstleistungen auch die räumlichen und zeitlichen Bedingungen der Kommunikation und Kooperation ändern und für viele Anwendungen die direkte Kommunikation oder die Nutzung nicht-elektronischer Kommunikationswege ausschließen. Schließlich könnten auch geänderte Sicherungsanforderungen zusätzliche Schäden verursachen: So könnte zum Beispiel Verschlüsselung in bestimmten Fällen vorgeschrieben sein, so dass ohne sichere Verschlüsselungssysteme nicht mehr kommuniziert werden darf. Dies würde die Abhängigkeit von Schlüsselinhabern erhöhen und diesen neue Mißbrauchsmöglichkeiten eröffnen. (Pordesch 1995).

Sicherungsstrategien

Das Internet und seine Dienste bieten wenig Grundsicherung. Von der dezentralen Struktur des Netzes her können zentrale Sicherungsansätze wahrscheinlich nur eine begrenzte Wirksamkeit entfalten. Der Grad an erreichbarer Sicherheit wird deshalb wesentlich von den Selbstschutzmaßnahmen der Anwender und lokaler Anbieter abhängen. Solche können beispielsweise liegen in

einer Weiterentwicklung von Firewalls,

dem individuellen Einsatz von Sicherungstechniken wie PGP und

individuellen Diversifizierungsstrategien wie die Nutzung mehrerer Provider und Zugangsnetze.

Es wäre zu untersuchen, welche weiteren Formen des Selbstschutzes möglich sind und ob diese unter Marktbedingungen zu einem ausreichenden Sicherungsniveau führen können. Interessant wäre es, die möglichen Maßnahmen einzelner Anwender und Anbieter abzuschätzen, die jenseits eines für bestimmte Risiken unzureichenden passiven Selbstschutzes verbleiben. Möglichkeiten zu einem „aktiven Selbstschutz" könnten liegen im

Boykott bestimmter Anwender und Anbieter,

aktiven Störungen und Gegenangriffen,

Überwachung des Verkehrs oder

öffentlichen Bloßstellungen.

Unabhängig davon wäre zu untersuchen, welche Sicherheitsgewährleistungen bei der marktförmigen, nicht zentral geplanten Entwicklung zu erwarten sind und welche Verletzlichkeitsprobleme dadurch nicht abgedeckt werden. Daraus ist abzuleiten, welche Maßnahmen Netzbetreiber und Anbieter ergreifen sollten, den Systemschutz technisch und organisatorisch zu verbessern, und welcher rechtlicher Regelungen es bedarf, Sicherungsmaßnahmen durchzusetzen.

Literatur

BSI (Hrsg.) (1995a): Chipkarten im Gesundheitswesen, Bonn 1995.

BSI (Hrsg.) (1995b): Informationstechnik zur Fahrerunterstützung im Straßenverkehr, Bonn 1995.

Hammer, V. (Hrsg.): Sicherungsinfrastrukturen - Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin 1995.

Mann, E. (1994): Desert Storm: The first information war?, Airpower Journal, Winter 1994, 4 ff.

National Research Council (NRC) (1989): Growing Vulnerability of the Public Switched Networks: Implications for National Security, Washington 1989.

Pordesch, U. (1989): Zum Katastrophenpotential der Telekommunikation, Zivilverteidigung, 20. Jg.(1989), Heft 2, 41 ff.

Pordesch, U. (1995): Gesellschaftliche Folgen von Sicherungsinfrastrukturen und Grenzen der Technikgestaltung, in: Hammer (1995), 247 ff.

Roßnagel, A. (1995): Die Verletzlichkeit der Informationsgesellschaft und rechtlicher Gestaltungsbedarf, in: Kreowski, H. J. u.a. (Hrsg.), Realität und Utopien der Informatik, Münster 1995, 56 ff.

Roßnagel, A. (1996): Die Infrastruktur sicherer und verbindlicher Telekooperation, Friedrich Ebert Stiftung, Bonn 1996.

Roßnagel, A. (1997): Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Bürger. Thesen zu einem neuen Verständnis der Staatsaufgaben in einer ‚civil information society‘, Zeitschrift für Rechtspolitik 1997, 26 ff.

Roßnagel, A. / Pordesch, U. (1989): Informationstechnische Vernetzung und Verteidigungsfähigkeit, Sicherheit und Frieden, 7. Jg. (1989), Heft 4, 220 ff.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990a): Die Verletzlichkeit der Informationsgesellschaft, 2. Auflage, Opladen 1990.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990b): Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.

SARK (1979): Datenverarbeitung und die Verwundbarkeit der Gesellschaft, Bericht des Verwundbarkeitskomitees, Stockholm 1979.

Die Entwicklung des Datenschutzes in Europa

Auszug aus einer Rede, die **Peter J. Hustinx**, Präsident der Registratiekamer, Niederlande, am 29.08.1994 in Kiel gehalten hat (mit Wirkung vom 17.01.2004 wurde er für 5 Jahre zum Europäischen Datenschutzbeauftragten ernannt)

Man hat mich gebeten, über die Entwicklung des Datenschutzes in Europa zu sprechen. Über das Thema nachdenkend, wurde mir klar, dass die heutige Situation auf dem Gebiet des Datenschutzes das Ergebnis einer etwa fünfundzwanzigjährigen Entwicklung ist, bei der Deutschland und einige skandinavische Länder, darunter vor allem Schweden, eine Pionierrolle gespielt haben. Aus diesem Grund erscheint es mir sinnvoll, diese Entwicklung in groben Zügen nachzuzeichnen und mit einigen Randbemerkungen zu versehen. Sodann werde ich auf den Entwurf einer diesbezüglichen EG-Richtlinie eingehen. Der Zufall will es, dass Deutschland dabei wiederum eine Hauptrolle spielt, da es zur Zeit den Vorsitz in der Europäischen Union führt. Im letzten Teil meiner Ausführungen werde ich versuchen, eine Bilanz zu ziehen und einen Blick in die Zukunft werfen.

Die soeben erwähnte Entwicklungsgeschichte von etwa fünfundzwanzig Jahren möchte ich in vier Phasen unterteilen. Während der ersten drei Phasen, etwa zwischen 1970 und 1990, lag die Führungsrolle in der Rechtsentwicklung auf europäischer Ebene eindeutig beim Europarat. In den letzten Jahren wurde sie von der europäischen Gemeinschaft, der heutigen Europäische Union, übernommen. Auf nähere Einzelheiten werde ich noch zu sprechen kommen.

Pionierzeit

Einer der ersten und größten Erfolge des Europarats war die Verabschiedung der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten. 1968 ersuchte die Parlamentarische Versammlung des Europarats das Ministerkomitee zu prüfen, ob die Konvention und das nationale Recht der einzelnen Mitgliedsstaaten angesichts der Entwicklung von Wissenschaft und Technik genügend Garantien für den Schutz der privaten Sphäre boten. Wie sich zeigte, ließ der Schutz im Bereich der automatischen Datenverarbeitung zu wünschen übrig. Aus diesem Grund nahm das Ministerkomitee 1973 und 1974 zwei Empfehlungen an, mit denen die Mitgliedsstaaten aufgefordert wurden, geeignete Maßnahmen zu ergreifen. Die erste Empfehlung enthielt eine Reihe von Richtlinien für den Datenschutz im Privatsektor, die zweite war dem öffentlichen Sektor gewidmet. In den beiden Empfehlungen war in Umrissen bereits das erkennbar, was später zum harten Kern, zu den Grundprinzipien des Datenschutzes zählen sollte. Die Empfehlungen sagten nichts über Art und Form der Maßnahmen aus, bauten jedoch auf den ersten nationalen Gesetzesinitiativen im Land Hessen (1970) und in Schweden (1973) auf.

Dass die Europäische Menschenrechtskonvention nur unzureichenden Schutz bot, erscheint aus heutiger Sicht kaum erstaunlich. Die Verarbeitung personenbezogener Daten befindet sich gleichsam an der Schnittfläche zweier Grundrechte: des Rechts auf Achtung der privaten Sphäre und des Rechts auf Informationsfreiheit. Das Verhältnis zwischen den beiden Rechten ist nicht ohne weiteres deutlich. Auch die Bestimmung der Reichweite des Rechts auf Achtung der privaten Sphäre bringt Probleme mit sich. Die bloße Tatsache, dass Daten personenbezogen sind, reicht nicht aus, sie unter den Wirkungsbereich des Grundrechts zu stellen. In den Entscheidungen des Europäischen Gerichtshofs für Menschenrechte geht es immer um besondere Situationen wie sensible Daten oder geheime Polizeikontrollen. Schließlich sieht die Konvention in erster Linie ein Abwehrrecht gegenüber dem Staat vor und bietet nur im beschränktem Maße Unterstützung in bezug auf positive Rechtsansprüche. Zur Verbesserung des Schutzes der Privatsphäre mussten daher andere Wege beschritten werden. Die Möglichkeit eines Zusatzvertrages wurde in der ersten

Hälfte der siebziger Jahre zwar erörtert, aber man fand, dass dafür die Zeit noch nicht reif war. Empfehlungen schienen rascher zum gewünschten Ziel zu führen.

Straßburger Vertrag

Einige Jahre später begann man dennoch mit den Vorbereitungen zu diesem Vertrag. Der Grund dafür war, dass man eine Reihe von Problemen auf dem Gebiet des internationalen Datenverkehrs nur über einen Vertrag zufriedenstellend lösen konnte. Im Jahre 1976 wurde ein Sachverständigenkomitee eingesetzt, das vier Jahre brauchte, um seine Arbeit zu vollenden. So kam schließlich der Straßburger Vertrag vom 28. Januar 1981 zustande[44]. Dieser Vertrag enthielt eine Reihe von Grundsätzen für den Datenschutz, denen jede Partei in ihrem nationalen Recht Rechnung zu tragen hatte, und zwar spätestens zu dem Zeitpunkt, zu dem der Vertrag für diese Partei in Kraft treten sollte. Darüber hinaus enthielt der Vertrag eine Regelung für den grenzüberschreitenden Datenverkehr, die im Prinzip auf eine völlige Liberalisierung des Datenverkehrs zwischen den Vertragsparteien hinauslief. Schließlich wurden Bestimmungen über die gegenseitige Unterstützung und die Einsetzung eines Beratenden Komitees aufgenommen, wodurch eine ordnungsgemäße Anwendung des Vertrages gewährleistet werden sollte. Eine Besonderheit war ferner, dass auch Nichtmitgliedern des Europarats die Möglichkeit geboten wurde, dem Vertrag beizutreten. Dies war durch eine gewisse Abstimmung mit der Arbeit im Rahmen der OECD ermöglicht worden, einer Organisation, der auch Länder wie Australien, Kanada und die Vereinigten Staaten angehören. Trotz ernsthafter Bemühungen in dieser Richtung konnte der Vertrag keine Lösung für Probleme auf dem Gebiet der Rechtsprechung und des anwendbaren Rechts bieten. Der Vertrag bestimmt hier lediglich, dass jede Partei verpflichtet ist, auf ihrem Hoheitsgebiet jeder natürlichen Person ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes, Datenschutz zu gewährleisten.

Die Vorbereitung des Vertrags ging mit einer starken Zunahme der Gesetzgebungstätigkeit auf nationaler Ebene einher. So kamen in dieser Zeit Gesetze in der Bundesrepublik, in Frankreich, Norwegen, Dänemark, Österreich und Luxemburg zustande; im Jahre 1984 schloß sich auch Großbritannien an, vor allem weil man fürchtete, ansonsten die Möglichkeit eines freien Datenverkehrs mit dem Rest Europas zu verlieren. Der Straßburger Vertrag trat nach seiner Ratifizierung durch fünf Länder am 1. Oktober 1985 in Kraft. Inzwischen sind dem Vertrag 15 Länder beigetreten. Von der Möglichkeit des Beitritts außereuropäischer Länder wurde noch kein Gebrauch gemacht.

Über den heutigen Wert des Straßburger Vertrags läßt sich streiten. Sein Zustandekommen war ohne Zweifel ein historisches Ereignis. Nach der Zahl der Ratifizierungen zu schließen, hat der Vertrag in weiten Kreisen Zustimmung gefunden. Manche haben sogar die Auffassung vertreten, dass auch in der Europäischen Union eine Ratifizierung des Vertrags durch alle Mitgliedstaaten ausreichen würde. Diese Auffassung wird jedoch nur noch von wenigen geteilt. Andererseits wird auch darauf hingewiesen, dass der Vertrag nicht mehr zeitgemäß und durch die technischen Entwicklungen überholt ist. Tatsächlich trägt der Vertrag in mancherlei Hinsicht die Spuren der Zeit, in der er entstand. Ich finde jedoch die Schlußfolgerung zutreffend, die Ende der achtziger Jahre in einem Bericht des Europarats gezogen wurde, nämlich dass die Begriffe und Grundsätze des Vertrags gerade durch die offene Formulierung ihre Zeit überdauert haben und daher noch immer wertvoll sind.

---

[44] Sie finden ihn im Anhang: Council of Europe: Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data.

Nähere Ausgestaltung

Nach dem Zustandekommen des Straßburger Vertrags seinen allgemeinen Grundprinzipien wurde innerhalb des Europarats der Nachdruck auf seine nähere Ausgestaltung in Form von Empfehlungen für die einzelnen Bereiche gelegt. Es ist nun einmal eine bekannte Tatsache, dass die Grundprinzipien des Datenschutzes nur bei einer bereichsspezifischen Ausgestaltung wirklich zum Tragen kommen. So entstanden unter anderem Empfehlungen über medizinische Daten, wissenschaftliche Forschung und Statistik, Direktvertrieb, soziale Sicherheit, Polizei, Arbeit und elektronischen Zahlungsverkehr. In allen Fällen kam es zu Neuentwicklungen, die die Rechtsentwicklung in den Mitgliedstaaten beeinflußten. Die Empfehlung über die Nutzung personenbezogener Daten im Polizeibereich wird im Schengener Durchführungsabkommen sogar als Richtlinie bezeichnet, der bei der Anwendung dieses Vertrags Rechnung getragen werden muss.

Auch auf der Ebene der Mitgliedstaaten gab es interessante Entwicklungen. So kamen in der zweiten Hälfte der achtziger Jahre in Finnland, Irland und in den Niederlanden neue Gesetze zustande. Dabei vollzog sich ein Umschlag zur sogenannten Gesetzgebung der zweiten Generation. Sie kennzeichnet sich unter anderem durch größere Flexibilität und niedrigere Verwaltungskosten. Auch Länder, die zu einem früheren Zeitpunkt Gesetze verabschiedet hatten, führten in dieser Zeit Vereinfachungen durch. Schweden war dafür ein typisches Beispiel.

Diese Entwicklungen brachten es mit sich, dass das Europa der Zwölf, die Europäische Gemeinschaft also, Ende der achtziger Jahre ein wechselndes Bild bot. In einigen Mitgliedstaaten, insbesondere den südlichen, waren noch keine Rechtsvorschriften zustande gekommen. In den Ländern, in denen dies wohl der Fall war, waren allerlei Unterschiede zu verzeichnen. Ein nicht unwichtiger dogmatischer Punkt war zum Beispiel, dass man sich in der Bundesrepublik inzwischen für das Recht auf informationelle Selbstbestimmung entschieden hatte. Ich meine hier das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983. In den Niederlanden wird dieser Gegenstand in der Verfassung etwas anders behandelt, und zwar ausgehend vom Grundrecht auf Wahrung der Privatsphäre, ergänzt durch einen Auftrag an den Gesetzgeber, Schutzmaßnahmen zu treffen. Im Vereinigten Königreich hat man wiederum die Neigung, das aktuelle Thema pragmatisch anzupacken und Verhaltensregeln für "faire Informationsverarbeitung" zu entwickeln. Es ist nützlich, sich diese Unterschiede vor Augen zu halten. Wichtiger als die dogmatischen Unterschiede sind jedoch die praktischen Unterschiede in der Ausgestaltung der Grundprinzipien des Straßburger Vertrags. So hat jedes Land seinen eigenen Mix von Regeln, Kontrollmaßnahmen, Strafverfolgungsmaßnahmen und dergleichen. In den meisten Fällen sind dafür gute Gründe anzuführen, die unter anderem auf unterschiedliche lokale Gegebenheiten und auf Unterschiede in der Rechtskultur zurückzuführen sind. Dadurch können jedoch Probleme bei der internationalen Zusammenarbeit und beim internationalen Datenverkehr entstehen.

Initiative der Europäischen Kommission

So sah also die Situation in Europa aus, als die Europäische Kommission Mitte 1990 einen Katalog von Maßnahmen vorlegte. Dazu gehörte der Vorschlag für eine EG-Richtlinie zur Harmonisierung des Datenschutzrechts der einzelnen Mitgliedstaaten. Dieser Vorschlag kam nicht ganz unerwartet. Vertreter der Kommission hatten fast von Anfang an an der Arbeit des Europarats teilgenommen und sich stets eigene Initiativen der Kommission vorbehalten. Trotz wiederholten Drängens des Europäischen Parlaments hatte sich die Kommission jedoch auf Empfehlungen an die Mitgliedstaaten, dem Straßburger Vertrag beizutreten, beschränkt. Da diese Empfehlungen nicht das gewünschte Resultat zeigten, sah sich die Kommission offensichtlich veranlaßt, selbst die Initiative zu ergreifen. Auch Appelle aus Kreisen der Datenschutzbeauftragten können hierzu beigetragen haben. Darüber hinaus war sich die Kommission vermutlich von der wachsenden

Bedeutung dieser Materie angesichts der Vollendung des gemeinsamen Binnenmarktes, insbesondere auf dem Gebiet der informationsintensiven Dienstleistungen, stärker bewußt geworden. Dies wurde noch durch die politische Bedeutung unterstrichen, die eine gute Regelung des Datenschutzes im Rahmen des Schengener Durchführungsabkommens hatte. In diesem Vertrag über die Zusammenarbeit zwischen einer Reihe von EG-Staaten auf dem Gebiet des Polizeiwesens und der Sicherheit spielt der Datenaustausch eine wichtige Rolle.

Der Vorschlag der Kommission beruht auf Artikel 100a des EG-Vertrags, die übliche Grundlage für Harmonisierungsrichtlinien in Fällen wie diesem. Dabei hatte die Kommission auf ein hohes Schutzniveau gesetzt, da die Mitgliedstaaten, die über einschlägige Rechtsvorschriften verfügten, nur so zur Aufgabe ihrer nationalen Arbeitsweise veranlaßt werden könnten. Zwar haben die Mitgliedsländer bei einer Richtlinie einen gewissen Handlungsspielraum, aber sie müssen sich an die Maßstäbe halten, die ihnen die Richtlinie auferlegt. Ferner sollte man bedenken, dass die Europäische Gemeinschaft nur über die Befugnisse verfügt, die ihr der EG-Vertrag überträgt. Eine Datenschutzregelung kann für sie daher nur ein Mittel im Dienste der Vollendung des Binnenmarktes sein. Allerdings ist auch die Gemeinschaft an die Rechtsgrundlagen gebunden, zu denen laut Europäischem Gerichtshof auch die in der Europäischen Menschenrechtskonvention verankerten Grundrechte gehören. Der Richtlinienentwurf beruhte daher auf dem Grundsatz, dass zumindest der Straßburger Vertrag einge-halten werden muss.

Der Entwurf aus dem Jahre 1990 wurde nicht sehr positiv aufgenommen. Es dürfte wenig Vorschläge gegeben haben, die mit soviel Kritik empfangen wurden, wie dieser Entwurf. Die Kritik kam aus nahezu allen Bereichen. Auch die Europäische Konferenz der Datenschutzbeauftragten hat auf Berichtigung gedrängt. Dies führte zu einer großen Zahl von Änderungsanträgen seitens des Europäischen Parlaments. Im Zusammenhang damit legte die Kommission 1992 einen stark geänderten Entwurf vor, der glücklicherweise noch immer auf denselben prinzipiellen Ausgangspunkten beruht. Auf der Grundlage dieses Entwurfs wird seither in einer Arbeitsgruppe des EG-Ministerrats verhandelt.

Europäische Datenschutzbeauftragte

Es spricht für sich, dass die europäischen Datenschutzbeauftragten auch den geänderten Text des Richtlinienentwurfs äußerst sorgfältig geprüft haben. In drei Plenarsitzungen von je zwei Tagen haben sie sich danach intensiv mit dem Entwurf auseinandergesetzt. Daraufhin formulierten sie einen gemeinsamen Standpunkt, der im Frühjahr 1993 der Europäischen Kommission, dem Europäischen Parlament und der Arbeitsgruppe des EG-Ministerrats vorgelegt wurde.

In diesem Papier erklären sich die Datenschutzbeauftragten zunächst mit dem Ziel der Richtlinie völlig einverstanden, die einen gleichwertigen Datenschutz in allen EC Ländern vorsieht, der den Grundsätzen des Straßburger Vertrags entspricht. Sie schließen sich dabei auch ganz der Auffassung der Kommission an, derzufolge die Harmonisierung der Rechtsvorschriften nicht zu einer Verringerung des heutigen Datenschutzes, sondern vielmehr zu einem hohen Niveau des Schutzes in der ganzen Gemeinschaft führen muss.

Vor diesem Hintergrund äußerten sie doch einige Besorgnis über die im Richtlinienentwurf angewendete Methode der Harmonisierung. Der Entwurf enthält nämlich ziemlich viele allgemeine Grundsätze, die einer näheren Auslegung und spezifischer Anwendung bedürfen. Dabei verfügen die Mitgliedstaaten über einen gewissen Spielraum, was zur Folge haben kann, dass manche Länder sich für eine strengere Interpretation entscheiden als andere. Dasselbe gilt für einen großen Teil der Ausnahmen, die der Richtlinienentwurf einem Mitgliedstaat zuerkennt. Dies alles kann dazu führen, dass es in der Praxis dennoch verschiedene Schutzniveaus gibt

Ich denke, dass wir es hier mit einem schwierigen Problem zu tun haben. Die Harmonisierung von Rechtsvorschriften ist immer eine Frage des Gebens und Nehmens. Das gilt auch für den

Bereich des Datenschutzes. Wenn man die Spielräume für nationale Unterschiede verringern will, dann wird man auf internationaler Ebene in mehr Details treten müssen. Dies stößt jedoch häufig auf so viele Probleme, dass eine gemeinsame Lösung unmöglich wird. Auch das Subsidiaritätsprinzip spielt hier natürlich eine große Rolle. Daher wird man kaum umhinkommen, gewisse Unterschiede im Hinblick auf eine nähere Abstimmung vorerst zu akzeptieren.

Unter diesen Umständen ist es von entscheidender Bedeutung, die Grenzen der Richtlinie sorgfältig zu bewachen, damit unnötige Differenzen vermieden werden können. Auch ist darauf zu achten, dass die Richtlinie in ihrer Gesamtheit ein ausreichend hohes Schutzniveau bietet. In diesem Zusammenhang enthielt das gemeinsame Papier der Datenschutzbeauftragten zahlreiche Vorschläge zur Verbesserung bestimmter Teile des Wortlauts der Richtlinie. Diese Vorschläge wurden dann auch in die Verhandlungen eingebracht. Noch kürzlich haben die Datenschutzbeauftragten ihr gemeinsames Papier vom letzten Jahr noch in einem entscheidenden Punkt ergänzt, nämlich in bezug auf die Problematik des anwendbaren Rechts. Darauf komme ich noch gesondert zurück.

Grundzüge des Richtlinienentwurfs

Zunächst noch einige Bemerkungen über die Grundzüge des Richtlinienentwurfs, wie er uns hier vorliegt. Allerdings will ich darauf hinweisen, dass die Verhandlungen noch laufen. Daher sind Änderungen im Entwurf noch möglich. Auch abgesehen davon, muss ich mir hier Beschränkungen auferlegen.

Der Kern des Richtlinienentwurfs ist der Auftrag an die Mitgliedstaaten, für einen Datenschutz zu sorgen, der den Anforderungen der Richtlinie entspricht. Dem steht gegenüber, dass sie den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten dann nicht mehr aus Gründen des Datenschutzes einschränken oder verbieten dürfen. Ich muss annehmen, dass diese Bestimmung nicht im Widerspruch zu Beschränkungen steht, die sich aus der Richtlinie selbst notwendigerweise ergeben wie etwa dem Verbot, Daten an Unbefugte zu übermitteln, gleichgültig, wo diese sich befinden. Auch kann eine Bestimmung wie diese nur innerhalb des Anwendungsbereichs der Richtlinie wirksam werden. Sie steht also eventuellen Beschränkungen im Zusammenhang mit Dateien, auf die die Richtlinie nicht anwendbar ist, nicht im Wege. Die Frage, ob die Richtlinie auch für nicht-automatisierte Dateien gelten soll, ist Gegenstand intensiver Diskussionen. Eine bejahende Antwort halte ich nicht für ausgeschlossen, wenngleich hier mit einer zusätzlichen Übergangsperiode zu rechnen ist.

Was die materiellen Bestimmungen in Sachen Datenverarbeitung angeht, lehnt sich der Richtlinienentwurf an den Straßburger Vertrag an. Darüber hinaus enthält der Entwurf eine Aufzählung der Fälle, in denen die Verarbeitung personenbezogener Daten erlaubt ist. In den Rechtsvorschriften der Mitgliedstaaten müssen diese Bestimmungen dann näher ausgearbeitet werden. Dies erfordert schließlich eine Abwägung der Interessen aufgrund der Besonderheiten des jeweiligen Einzelfalls. Ich denke, dass die Richtlinie in diesem Teilbereich wenig mehr bieten kann und dass eine nähere Ausgestaltung auf der Ebene der Mitgliedstaaten erfolgen muss. Der Richtlinienentwurf enthält allerdings noch eine Regelung für die Verarbeitung sensitiver Daten, wie zum Beispiel Angaben über die Religionszugehörigkeit, die politische Überzeugung, die Abstammung und ähnliches. Völlig klar ist, dass auf diesem Gebiet besondere Garantien erforderlich sind. Aufgrund meiner Erfahrungen in den Niederlanden neige ich mehr zu einer schärferen Abwägung als zu strengen Verboten. Die Praxis ist hier schließlich weit differenzierter als man zunächst annehmen möchte.

Die Bestimmungen über die Rechte der Betroffenen haben Anlaß zu Kritik von verschiedenen Seiten gegeben: zuviel Papierkram und ein Mangel an tatsächlichem Schutz! Soweit diese Kritik gerechtfertigt war, hat man sie sich inzwischen zu Herzen genommen. Ich hielte es für unvernünftig, wenn man das rechte Verhältnis zwischen Kosten und Nutzen in einem Bereich wie

diesem aus den Augen verlöre. Was nunmehr vorliegt, kann der Kritik durchaus standhalten. Das gilt sicherlich auch für Einwände seitens der Absatz- und Werbewirtschaft. Ich bin davon überzeugt, dass mehr Transparenz auf diesem Gebiet dringend notwendig ist und dass der Richtlinienentwurf einer ausgewogenen Entwicklung nicht im Wege zu stehen braucht.

Eine ähnliche Abwägung gilt für die Bestimmungen über die Meldung bei den Aufsichtsbehörden. Es erscheint mir gut vertretbar, die Meldepflicht bei der Verarbeitung von Daten als Grundregel voranzustellen. Aber von dieser Grundregel sollte es weitreichende Ausnahmen geben. Wenn ich recht sehe, dann entscheidet man sich jetzt für ein System der Freistellung mit einer Wahlmöglichkeit: Entweder aufgrund genau umschriebener Kategorien von Verarbeitungen oder aufgrund einer unabhängigen Aufsicht innerhalb der betreffenden Organisation, wie man sie in Deutschland bereits kennt. Obwohl für mich nicht ganz klar ist, wie ein solches System auf europäischer Ebene arbeiten wird, bietet dieses Vorgehen interessante Perspektiven. Ich reagiere also mit gewissem Vorbehalt positiv.

Was den weiteren Inhalt des Richtlinienentwurfs angeht, gestatten Sie mir noch zwei kurze Bemerkungen über die Aufsichtsbehörden. Ich halte es für sehr wichtig, dass die Richtlinie mindestens eine unabhängige aufsichtsführende Instanz vorsieht. Im Straßburger Vertrag war darüber nichts zu finden. Seither ist die Aufsicht als wesentliche Voraussetzung anerkannt worden. Die Richtlinie gibt ferner genau an, welche Befugnisse die Aufsichtsbehörde besitzen muss. Ich denke, dass die Richtlinie genügend Raum für verschiedene Traditionen bietet, solange eine wirksame Aufsicht hinreichend gewährleistet ist.

Anwendbares Recht

Der Richtlinienentwurf enthält auch eine Bestimmung über eine diffizile Materie, die für die Praxis große Folgen haben kann: die Frage, welches nationale Recht in einem bestimmten Fall anwendbar ist. Die vorgeschlagene Regelung beinhaltet, kurz gesagt, dass im Falle von Datenverarbeitungen innerhalb der Europäischen Gemeinschaft das Recht des Landes gilt, in dem der verantwortliche Halter seinen Sitz hat. Solange alle relevanten Anknüpfungspunkte der Verarbeitung sich auf einen einzigen Mitgliedstaat beziehen, wird diese Bestimmung kaum Folgen haben. Beim internationalen Datenverkehr ist das jedoch anders. Das bedeutet, dass künftig in jedem Mitgliedstaat ausländisches Recht anwendbar sein kann und immer häufiger auch anwendbar sein wird. Demzufolge wird der Datenschutz in einem bestimmten Land auch von ausländischen Gesetzgebern und von den Aktivitäten ausländischer Aufsichtsbehörden abhängig sein.

Die europäischen Datenschutzbeauftragten haben in ihrem gemeinsamen Papier Einwände gegen dieses Teil des Richtlinienentwurfs erhoben und eine erneute Prüfung gefordert. Seither haben sie sich auch selbst weiter in diese Materie vertieft. Das hat zu einer Ergänzung ihres gemeinsamen Papiers geführt, die der Europäischen Kommission und dem EG-Ministerrat kürzlich zur Kenntnis gebracht worden ist. In Ihrem Brief weisen die europäischen Datenschutzbeauftragten darauf hin, dass die angezeigte Problematik eng mit dem Umstand zusammenhängt, dass es auch in Zukunft nicht unbedeutende Unterschiede zwischen den Rechtsvorschriften der Mitgliedstaaten geben wird. Bei der Suche nach einer Lösung für diese Problematik muss einem guten Rechtsschutz der Bürger und der Möglichkeit zur Ausübung einer wirksamen Aufsicht stets Vorrang eingeräumt werden. Die vorgeschlagene Regelung muss daher auf jeden Fall in einigen Punkten angepaßt werden.

So müssen die Aufsichtsbehörden tätig werden können, egal ob ihr eigenes materielles Recht anwendbar ist oder nicht. Das heißt, dass sie die Einhaltung ausländischen Rechts innerhalb ihres Zuständigkeitsbereiches kontrollieren und, falls erforderlich, eingreifen können müssen. Demnach müssen die Mitgliedstaaten also auch für geeignete Rechtsmittel und Sanktionen sorgen, damit sie bei Verstößen gegen ausländisches Recht auf ihrem Hoheitsgebiet tätig werden können. Aber auch

das materielle Recht des Ortes der Verarbeitung muss in bestimmten Situationen anwendbar bleiben. Das gilt sicherlich für die Regeln in Sachen Sicherheit, aber auch in Fällen, in denen schwerwiegende Gründe des öffentlichen Interesses ("ordre public") hierzu Anlaß geben. Im letzteren Fall ist unter anderem an Regeln über die Verarbeitung sensibler Daten zu denken. Ich hoffe, dass diese dringenden Empfehlungen in den kommenden Monaten beachtet werden.

Zukunftsaussichten

Damit bin ich beim heutigen Stand der Dinge und bei den Perspektiven für die Zukunft angelangt. Die Verhandlungen über den Richtlinienentwurf in der Arbeitsgruppe des Rats befinden sich in einem entscheidenden Stadium. Das könnte bedeuten, dass noch dieses Jahr ein gemeinsamer Standpunkt formuliert werden kann. Nach den heutigen Spielregeln würde die Richtlinie dann möglicherweise in der zweiten Hälfte des nächsten Jahres zustande kommen. Möglicherweise werden die Mitgliedstaaten dann bis zwei Jahre Zeit bekommen, um ihre Rechtsvorschriften mit dem Inhalt der Richtlinie in Einklang zu bringen. Das bedeutet, dass die geplante Harmonisierung im Jahre 1998 erfolgen könnte. Für bestehende Systeme wird dann wahrscheinlich eine Übergangsperiode gelten. Eine solche Übergangsperiode, wird es, wie bereits gesagt, auch für nicht-automatisierte Dateien geben.

Dies alles bedeutet, dass es in den nächsten Jahren noch eine ganze Menge Arbeit zu tun gibt. Das gilt für die Durchführung der Richtlinie auf nationaler Ebene, aber auch für die europäische Zusammenarbeit. Die Richtlinie sieht zu diesem Zweck unter anderem die Einsetzung einer Arbeitsgruppe mit Vertretern der nationalen Aufsichtsbehörden vor. Die immer intensivere Zusammenarbeit zwischen unseren Einrichtungen in den verschiedenen Mitgliedsländern könnte dann in diesem Rahmen fortgesetzt werden. Aufgrund meiner heutigen Erfahrungen habe ich hierin volles Vertrauen, auch wenn der Kreis der Länder — durch das Inkrafttreten der Richtlinie oder durch den Beitritt neuer Mitgliedstaaten— größer wird. Kollegen aus Portugal und Spanien haben unseren Kreis kürzlich erweitert, und mit den Kollegen aus den neuen Mitgliedstaaten besteht bereits seit Jahren eine gute Zusammenarbeit. Ich denke, dass die Arbeitsgruppe einen wichtigen Beitrag zur weiteren Entwicklung des Datenschutzes in Europa und zur gegenseitigen Abstimmung der Rechtsvorschriften in den Mitgliedstaaten leisten kann.

Vor diesem Hintergrund möchte ich noch drei Wünsche aussprechen. Der erste ist, dass wir nicht nur eine gute Richtlinie als allgemeinen Rahmen für die Entwicklung des Datenschutzes in Europa erhalten mögen, sondern auch gute und ausgewogene Maßnahmen in Teilbereichen, von denen die Telekommunikation zur Zeit am aktuellsten ist. In anderen Teilbereichen der europäischen Politik ist der Datenschutz häufig weniger überzeugend. Auf manchen Gebieten fehlt er sogar fast völlig. Ich denke dabei insbesondere an spezifische Maßnahmen, die Folgen für den Datenschutz haben können, wie zum Beispiel Maßnahmen gegen den Schwindel mit EG-Subventionen. Dabei ist für die EG-Einrichtungen selbst noch kein ausreichender Datenschutz vorhanden, ein Mangel, der immer problematischer wird. Aus unserem Kreis wurde bereits wiederholt Abhilfe gefordert, und ich weiß, dass an entsprechenden Maßnahmen gearbeitet wird. Schließlich möchte ich noch die Hoffnung aussprechen, dass man sich auch bei der europäischen Zusammenarbeit auf dem Gebiet des Polizeiwesens und der Sicherheit die Notwendigkeit eines guten Datenschutzes immer vor Augen hält. Im Schengener Durchführungsabkommen ist der Datenschutz sorgfältig geregelt. Nunmehr gilt es, dem guten Beispiel auch auf anderen Gebieten, wie Europol, zu folgen.

Council of Europe[45]: Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data

Council of Europe, European Treaty Series No. 108.

Signed January 28, 1981

Entered into force October 1, 1985

The Member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

CHAPTER I -- GENERAL PROVISIONS

Article 1 Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2 Definitions

For the purposes of this convention:

a. "personal data" means any information relating to an identified or identifiable individual ("data subject");

b. "automated data file" means any set of data undergoing automatic processing;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

---

[45] *Council of Europe* auf Deutsch *Europarat*; nicht zu verwechseln mit *Council of the European Union* auf Deutsch *Rat der Europäischen Union*

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3 Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions.

Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraph 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II - BASIC PRINCIPLES FOR DATA PROTECTION

Article 4 Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5 Quality of data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11 Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects of wider measure of protection than that stipulated in this convention.

CHAPTER III -- TRANSBORDER DATA FLOWS

Article 12 Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

CHAPTER IV -- MUTUAL ASSISTANCE

Article 13 Co-operation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this convention.
2. For that purpose:

a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority. 3. An authority designated by a Party shall at the request of an authority designated by another Party:

a. furnish information on its law and administrative practice in the field of data protection;

b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 Assistance to data subjects resident abroad

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating inter alia to:

a. the name, address and any other relevant particulars identifying the person making the request;

b. the automated personal data file to which the request pertains, or its controller;

c. the purpose of the request.

Article 15 Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16 Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

b. the request does not comply with the provisions of this convention

c. compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17 Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER V -- CONSULTATIVE COMMITTEE

Article 18 Composition of the committee

1. A Consultative Committee shall be set up after the entry into force of this convention.

2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19 Functions of the committee

The Consultative Committee:

a. may make proposals with a view to facilitating or improving the application of the convention;

b. may make proposals for amendment of this convention in accordance with Article 21;

c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;

d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20 Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI -- AMENDMENTS

Article 21 Amendments

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII -- FINAL CLAUSES

Article 22 Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23 Accession by non-member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24 Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25 Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26 Denunciation

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27 Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession

c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24;

d. any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

Weitere Originaltexte von Kodizes

ASIS Code of Ethics for Information Professionals

(ASIS = American Society for Information Science)

Proposed Revision by Thomas J. Froehlich
Current Draft before Board February, 1992

ASIS recognizes the plurality of uses and users of information technologies, services, systems and products and the diversity of goals or objectives, sometimes conflicting, among vendors, producers, mediators, and users of information systems. ASIS mandates high standards for its members, identifying the following areas of responsibility:

Responsibility to Employers / Clients / System Users

To act faithfully for their employers or clients in professional matters;

To uphold each user's, provider's or employer's rights to privacy and confidentiality an shall respect whatever proprietary rights belong to them:

by minimizing data collected about clients, patrons, or users, and by limiting access to, providing proper security for and ensuring proper disposal of such data insofar as it does not conflict with proper goals and constraints of their organizations,

by not disclosing information obtained during confidential interviews, except when such disclosure is mandated by law or in accord with proper policies of their employers or the proper rights of their clients.

To treat fairly all persons regardless of race, religion, sex, sexual orientation, age or national origin.

Responsibility to the Profession

To truthfully represent themselves and the information systems which they utilize or which they represent:

by not knowingly making false statements of providing erroneous information or fail to inform clients, sponsors, or employers of the limitations, conditions and constraints of the system,

by informing their employers, clients, or sponsors of any circumstances that could lead to a conflict of interest,

by not using their position beyond their authorized limits or by not using their credentials to misrepresent themselves.

To be and to remain competent and qualified, and to foster competence and deter incompetence among fellow professionals:

by only undertaking assignments for which they are qualified, and for which there is reasonable expectation of meeting requirements in a timely fashion,

by following and promoting standards of conduct in accord with the best current practices,

by undertaking their research conscientiously: in gathering, tabulating or interpreting data; in proper approval procedures for human subjects; or producing or disseminating to do the same,

by performing services in a manner that enhances or does not discredit the profession,

by adhering to principles of due process and equality of opportunity in peer relationships or personnel action.

Responsibility to Society

To improve, to the best of their means and abilities, the information systems in which they work or which they represent:

by resisting all forms of censorship, inappropriate selection and acquisition policies, and biases in information selection, provision and dissemination and by striving to correct errors or remedy biases and inaccuracies in information systems,

by making known any biases, errors and inaccuracies which exist and can not be or have not been remedied,

by providing the most reliable and accurate information and the degree of credibility of the sources as known or unknown.

To promote free and equal access to information, within the scope permitted by their organizations or work, and to resist procedures that promote discriminatory practices in access to and provision of information:

by seeking to extend public appreciation and awareness of information availability and provision and the role of information professionals in providing such information,

by freely reporting, publishing or disseminating information, subject to legal and proprietary restraints of vendor producer and employers, and the best interests of their employers, or clients.

Information professionals shall engage in principled conduct whether on their own behalf or at the request of employers, colleagues, clients, agencies or the profession: unprincipled conduct shall be challenged or disclosed.

BCS Code of Conduct

(BCS = The British Computer Society)

[BCS1] und [IFIP92](Auszug)

1. FOREWORD

The Society, through its Professional Advisory Committee, is ready all times to give guidance on the application of the Code of Conduct, and any member needing clarification or amplification of his or her obligation for the proper observance of professional conduct should seek the Committee's assistance.

In cases where it is considered that a member's conduct may have been in breach of the Code of Conduct and where informal resolutions of the matter is not possible, the Society's disciplinary procedures are described in this document.

2. CODE OF CONDUCT

Professional Conduct
Member's conduct shall uphold the dignity, reputation and good standing of the profession.

Professional Integrity
A member shall not by unfair means do anything that would harm the reputation, business or prospects of another member, and he shall at all times act with integrity towards the Society, its members and the members of other professions with whom he may be concerned in a professional capacity.

Public Interest
A member in discharging his responsibility to his employer or client shall have proper regard to the public interest and to the rights of third parties and, in particular, shall ensure that the intellectual property rights of others are not prejudiced by him.

Fidelity
A member shall discharge his obligation, to his employer or client with complete fidelity. He shall not disclose confidential information relating to his employer or client.

Technical Competence
A member shall offer only those services which are within his competence and shall declare to his employer or client the relevant level of competence he possesses when his services are being sought.

Impartiality
A member, when acting for a client, shall inform hi client in writing of any interest he may have which could prejudice the impartiality of hi, advice or could conflict with his client's interests.

3. DEFINITIONS/TERMINOLOGY

The following conventions apply to the reading of this code, and the notes for guidance.

1. "He" (etc) includes "She" (etc).

2. "Client" means any person, firm, company or other organization employing the member in an advisory capacity remunerated by fees.

3. Employer means any person, firm, company or other organization employing the member in a salaried position whether full-time or part-time.

4. User' is any person, department or organization served by computer-based systems.

5. "System" means all applications involving the use of computers. The term does not imply any particular mode of processing (e.g. dedicated, batch or transaction. "System may be interpreted as encompassing non-computer procedure such as clerical, manual, communication and electromechanical processes.

DPMA Code of Ethics

(DPMA = Data Processing Managers Association)

I acknowledge:

1. That I have an obligation to management, therefore, I shall promote the understanding of information processing methods and procedures to management using every recourse at my command.

2. That I have an obligation to my fellow members, therefore I shall uphold the high ideals of DPMA as outlined in its Association Bylaws. Further, I shall cooperate with my fellow members and shall treat them with honest and respect at all times.

3. That I have an obligation to society and will participate to the best of my ability in the dissemination of knowledge pertaining to the general development and understanding of information processing. Further, I shall nit use knowledge of a confidential nature to further my personal interest, nor shall I violate the privacy and confidentiality of information entrusted to me or to which I may gain access.

4. That I have an obligation to my employer whose trust I hold, therefore I shall endeavour to discharge this obligation to the best of my ability, to guard my employer's interests, and to advise him or her wisely and honestly.

5. That I have an obligation to my country, therefore, in my personal business and social contacts, I shall uphold my nation and shall honor the chosen way of life of my fellow citizens.

I accept these obligations as a personal responsibility, and as a member of this Association. I shall actively discharge these obligations and I dedicate myself to that end.

Ethische Leitlinien der GI[46] (von 1994)

Präambel

Das Handeln von Informatikerinnen und Informatikern steht in Wechselwirkung mit unterschiedlichen Lebensformen und -normen, deren besondere Art und Vielfalt sie berücksichtigen sollen und auch wollen. Dementsprechend sind diese Leitlinien nicht nur ethische Forderungen; sie sind zugleich Ausdruck des gemeinsamen Willens, diese Wechselwirkungen als wesentlichen Teil des eigenen individuellen und institutionellen beruflichen Handelns zu betrachten. Der offene Charakter dieser Forderungen wird mit dem Begriff Leitlinien unterstrichen.

Die Gesellschaft für Informatik e.V. (GI) will mit diesen Leitlinien bewirken, dass berufsethische Konflikte Gegenstand gemeinsamen Nachdenkens und Handelns werden. Ihr Interesse ist es, ihre Mitglieder, die sich mit verantwortungsvollem Verhalten exponiert haben, zu unterstützen. Vor allem will sie den Diskurs über ethische Fragen in der Informatik mit der Öffentlichkeit aufnehmen und Aufklärung leisten.

Handlungsalternativen und ihre absehbaren Wirkungen fachübergreifend zu thematisieren, ist in einer vernetzten Welt eine notwendige Aufgabe; hiermit sind einzelne zumeist überfordert. Deshalb hält es die GI für unerläßlich, die Zusammenhänge zwischen individueller und kollektiver Verantwortung zu verdeutlichen und dafür Verfahren zu entwickeln. Im Sinne dieser Ausführungen bindet sich die GI an die folgenden Leitlinien (§ 2.3 der Satzung der GI).

I Das Mitglied

Art. 1: Fachkompetenz

Vom Mitglied wird erwartet, dass es seine Fachkompetenz nach dem Stand von Wissenschaft und Technik ständig verbessert.

Art. 2: Sachkompetenz

Vom Mitglied wird erwartet, dass es sich über die Fachkompetenz hinaus in die seinen Aufgabenbereich betreffenden Anwendungen von Informatiksystemen soweit einarbeitet, dass es die Zusammenhänge versteht. Dazu bedarf es der Bereitschaft, die Anliegen und Interessen der verschiedenen Betroffenen zu verstehen und zu berücksichtigen.

Art. 3: Juristische Kompetenz

Vom Mitglied wird erwartet, dass es die einschlägigen rechtlichen Regelungen kennt, einhält und an ihrer Fortschreibung mitwirkt.

Art. 4: Kommunikative Kompetenz und Urteilsfähigkeit

Vom Mitglied wird erwartet, dass es seine Gesprächs- und Urteilsfähigkeit entwickelt, um als Informatikerin oder Informatiker an Gestaltungsprozessen und interdisziplinären Diskussionen im Sinne kollektiver Ethik mitwirken zu können.

---

[46] Diese ethischen Leitlinien wurden im Herbst 1994 in einer schriftlichen Abstimmung aller GI-Mitglieder bei ca. 25% Wahlbeteiligung mit 3506 (Zustimmung) zu 412 (Enthaltung) zu 468 (Ablehnung) angenommen. Kommentare zu diesen Leitlinien in: Christiane Floyd: Führen die Ethischen Leitlinien zu einer anderen Informatik? informatik magazin 6/94, Seite 9-10 und Karl-Heinz Rödiger, Rudolf Wilhelm: Zu den Ethischen Leitlinien der Gesellschaft für Informatik; Informatik-Spektrum 19/2 (1996) Seite 79-86.

II Das Mitglied in einer Führungsposition

Art. 5: Arbeitsbedingungen

Vom Mitglied in einer Führungsposition wird zusätzlich erwartet, dass es für Arbeitsbedingungen Sorge trägt, die es Informatikerinnen und Informatikern erlauben, ihre Aufgaben am Stand der Technik kritisch zu überprüfen.

Art. 6: Beteiligung

Vom Mitglied in einer Führungsposition wird zusätzlich erwartet, dass es dazu beiträgt, die von der Einführung von Informatiksystemen Betroffenen an der Gestaltung der Systeme und ihrer Nutzungsbedingungen angemessen zu beteiligen. Von ihm wird insbesondere erwartet, dass es keine Kontrolltechniken ohne Beteiligung der Betroffenen zuläßt.

Art. 7: Organisationsstrukturen

Vom Mitglied in einer Führungsposition wird zusätzlich erwartet, aktiv für Organisationsstrukturen und kommunikative Verfahren einzutreten, welche die Wahrnehmung von Verantwortung im Sinne kollektiver Ethik ermöglichen.

III Das Mitglied in Lehre und Forschung

Art. 8:

Vom Mitglied, das Informatik lehrt, wird zusätzlich erwartet, dass es die Lernenden auf deren Verantwortung sowohl im individuellen als auch im kollektiven Sinne vorbereitet und selbst hierbei Vorbild ist.

IV Die Gesellschaft für Informatik

Art. 9: Zivilcourage

Die GI ermutigt ihre Mitglieder in Situationen, in denen deren Pflichten gegenüber ihrem Arbeitgeber oder einem Kunden im Konflikt zur Verantwortung gegenüber Betroffenen stehen, mit Zivilcourage zu handeln.

Art. 10: Mediation

Die GI übernimmt Vermittlungsfunktionen, wenn Beteiligte in Konfliktsituationen diesen Wunsch an sie herantragen.[47]

Art. 11: Interdisziplinäre Diskurse

Die GI ermöglicht interdisziplinäre Diskurse zu ethischen Problemen der Informatik; die Auswahl der Themen wird selbst in solchen Diskursen getroffen. Vorschläge hierzu können einzelne Mitglieder und Gliederungen der GI machen. Die Ergebnisse der Diskurse werden veröffentlicht.

Art. 12: Fallsammlung

Die GI legt eine allgemein zugängliche Fallsammlung über ethische Konflikte an, kommentiert und aktualisiert sie regelmäßig.

---

[47] Wurde meines Wissens bisher nicht praktiziert. Angemerkt sei: IEEE hat eine Hotline zur Beratung der Mitglieder in berufsethischen Fragen nach einem guten Jahr Versuchsdauer und guten Erfahrungen damit (aus Sicht der die Hotline Betreibenden) Ende 1997 gegen deren Wunsch geschlossen, da das IEEE Executive Committee Bedenken wegen rechtlichen Haftungsfragen hatte (entnommen: The Institute, June 1998, Seite 2).

Art. 13: Präsidium
Die ethischen Leitlinien unterstützen das Präsidium (§ 9 der GI-Satzung) in seinen Aufgaben und Entscheidungen.

Art. 14: Fortschreibung
Die ethischen Leitlinien werden regelmäßig überarbeitet (§ 2.3 der Satzung der GI).

Erläuterungen

Betroffener
Der Begriff wird in den Datenschutzgesetzen definiert als die natürliche Person, über die Daten etwas auszusagen. Er umfaßt sowohl organisationsinterne (Beschäftigte, Nutzer) als auch organisationsex–terne Personen (Bürger, Kunden). Es empfiehlt sich, diesen eingebürgerten Bergriff für jegliche Form des Einsatzes von Informatiksystemen zu übernehmen. Die im englischen Sprachraum gebräuchliche Unterscheidung von "user" (intern) und "usee" (extern) hat sich in Deutschland bis jetzt nicht durchsetzen können.

Diskurs
Diskurse sind Verfahren gemeinschaftlicher Reflexion von Problemen mit einen normativen, d.h. wertbezogenen Hintergrund, die vom einzelnen oder einer einzelnen Fachdisziplin nicht überschaut werden können. Ihre wesentliche Leistung liegt darin, in der fachübergreifenden Kommunikation Erkenntnis- und Verständigungsgrenzen zu überwinden sowie Vor-Urteile zu hinterfragen und im Licht anderer Positionen zu rechtfertigen oder zu modifizieren, um Verständigung zu ermöglichen. Allein die Überwindung der Sprachbarrieren erweist sich als langwieriges Problem. Deshalb sollen Diskurse auf eine mittelfristige Dauer angelegt sein.

Fallsammlung
Unter Fallsammlung wird eine Zusammenfassung von Wirklichen Begebenheiten verstanden, in denen Beschäftigte (vorzugsweise Informatikerinnen und Informatiker) durch die ihnen übertragenen Aufgaben in ethische Konflikte geraten sind. Die zuständige Gliederung der GI wird diese Fälle zusammentragen und kommentieren. Die Sammlung hat den Sinn, diese Leitlinien zu konkretisieren und sie anhand praktischer Beispiele besser vermittelbar zu machen. Einzelne können diese Beispiele in vergleichbaren Situationen als Leitlinie für ihr Verhalten zu Rate ziehen.

Informatiksystem
Unter einem Informatiksystem wird die Einheit von Hard-, Software und Netzen einschließlich aller durch sie intendierten oder verursachten Gestaltungs- und Qualifizierungsprozesse bzgl. Arbeit und Organisation verstanden.

Kollektive Ethik
Ethik befaßt sich mit dem vorbedachten Verhalten von Menschen, die die Folgen ihres Verhaltens für andere Menschen, ihre Mitgeschöpfe und die Umwelt in noch unerfahrenen, durch Sitten und Rechtsnormen noch nicht geprägten Situationen bedenken (reflektieren). Hierbei können die Folgen des Verhaltens unmittelbar oder über längere Zeiten und größere Räume zu bedenken sein. Was der einzelne Mensch hinsichtlich dieser Verhaltensfolgen bedenken kann, umfaßt die individuelle Ethik.

Für den einzelnen Menschen sind aber nicht immer die Folgen von Verhalten in Kollektiven (Organisationen, Gruppen, Wirtschaften und Kulturen) überschaubar. Kollektives Verhalten bedarf

deshalb zusätzlich zur individuellen oder kollektiven Reflexion. Kollektive Ethik beruht auf der Möglichkeit, mit "Vorsicht" künftige kollektive Handlungen, die sich nicht an Erfahrungen und daraus entwickelten Normen orientieren können, gemeinschaftlich zu bedenken. Eine besondere Notwendigkeit solcher Reflexion ergibt sich immer dann, wenn individuelle Ethik oder Moral mit der kollektiven Ethik in Konflikt geraten.

Kontrolltechnik
Unter Kontrolltechnik werden analog zum Betriebsverfassungsgesetz "technische Einrichtungen" verstanden, die objektiv geeignet sind, "das Verhalten oder die Leistung der Arbeitnehmer zu überwachen" (§ 87 Abs. 1 Nr. 6 BetrVG). Bei der Einführung solcher Systeme steht den Interessenvertretungen ein Mitbestimmungsrecht zu.

Mediation
Unter Mediation werden Verhandlungsprozesse verstanden, mit deren Hilfe Interessenkonflikte zwischen zwei oder mehreren Parteien unter Hinzuziehung eines neutralen Dritten (Mediator) beigelegt werden. Das Ziel sind Problemlösungen, die von allen am Prozeß Beteiligten akzeptiert werden. Der Mediationsprozeß ist durch die Suche nach neuen Lösungen gekennzeichnet. Die Ergebnisse sind nicht rechtlich verpflichtend; als erfolgreich erweisen sich allgemein "jeder-gewinnt-Lösungen".

Rechtliche Regelungen
Rechtliche Regelungen, die für die Gestaltung von Informatiksystemen bedeutsam sind, finden sich inzwischen an zahlreichen Stellen der Rechtsordnung. Die wichtigsten sind:

- Allgemeiner und bereichsspezifischer Datenschutz, einschließlich Arbeitnehmerdatenschutz
- Freedom of information - Gesetzgebung (Informationszugangsgesetze, z.B. für den Umweltbereich)
- Computerstrafrecht
- Gewerblicher Rechtsschutz, insbesondere Urheber- und Patentrecht
- Allgemeine zivilrechtliche und strikte Produkthaftung
- IT-Sicherheitsrecht
- Telekommunikationsrecht.

In vielen, bei weitem aber nicht allen Fällen begründet die Einhaltung technischer Normen und Standards (DIN, EN, ISO) die Vermutung der Rechtstreue.

Stand von Wissenschaft und Technik
Die Leitlinien wären schon bei ihrer Verkündung veraltet, wenn man sich auf einen schon bekannten Wissensfundus in der Informatik bezöge. Statt starrer Verweise bietet sich als Ausweg an, das Prinzip der sog. offenen normativen Standards zu übernehmen, für das sich das deutsche technische Sicherheitsrecht entschieden hat. Das Bundesverfassungsgericht hat dieses Prinzip in mehreren Grundsatzentscheidungen zu einer sog. "Dreistufenlehre" konkretisiert (BVerfGE 49, 88 ff., BVerfGE 53, 30 ff., BVerfGE 56, 54 ff.):

1. Stufe: Allgemein anerkannte Regeln der Technik
Eine Regel ist dann allgemein anerkannt, wenn die herrschende Meinung der Praktiker eines Fachgebiets von ihrer Richtigkeit überzeugt ist und dies auch dokumentiert hat. Die Regel muss in der Fachpraxis bewährt und erprobt sein. Maßgebend ist die Durchschnittsmeinung der Praktiker, abweichende Auffassungen von Minderheiten sind unerheblich. Eine starke faktische Vermutung

für die allgemeine Anerkennung besteht, wenn z. Bsp. DIN- oder ISO-Normen für das Problem existieren.

2. Stufe: Stand der Technik
Der Maßstab für das Gebotene wird an die Front der technischen Entwicklung verlagert, für die die allgemeine Anerkennung und die praktische Bewährung alleine nicht ausreicht. Bei dieser Formel müssen Meinungsverschiedenheiten unter technischen Praktikern ermittelt werden. Die meisten Datenschutzgesetze enthalten in ihren Datensicherungsvorschriften einen Hinweis auf den "Stand der Technik (und Organisation)".

3. Stufe: Stand von Wissenschaft und Technik
Mit der Bezugnahme auf diese Formel wird ein noch stärkerer Zwang dahin ausgeübt, dass eine Regel mit der wissenschaftlichen und technischen Entwicklung Schritt hält. Geboten ist, was nach neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird. Das jeweils Erforderliche wird also nicht durch das technisch gegenwärtig Machbare begrenzt. Einen Verweis auf den "Stand von Wissenschaft und Technik" enthält z.B. das Produkthaftungsgesetz von 1989, das zumindest für Standardsoftware anwendbar ist. Es bietet sich an, an die Fachkompetenz der Informatiker besonders hohe Maßstäbe anzulegen (3. Stufe). Bei der Realisierung von Informatiksystemen müßte es im allgemeinen ausreichen, die Erwartungen, wie sie z.B. Datenschutzgesetze an Informatiker haben, jedenfalls nicht zu unterschreiten.

IEEE Code of Ethics (von 1975)

(IEEE = Institute of Electrical and Electronics Engineers, gegründet 20er Jahre, ≈ 330000 Mitglieder)

Preamble:

Engineers, scientists and technologists affect the quality of life for all people in our complex technological society. In the pursuit of their profession, therefore, it is vital that IEEE members conduct their work in an ethical manner so that they merit the confidence of colleagues, employers, clients and the public. This IEEE Code of Ethics represents such a standard of professional conduct for IEEE members in the discharge of their responsibilities to employers, to clients, to the community, and to their colleagues in this Institute and other professional societies.

Article I. Members shall maintain high standards of diligence, creativity and productivity, and shall:

a. Accept responsibility for their actions;
b. Be honest and realistic in stating claims or estimates from available data;
c. Undertake technological tasks and accept responsibility only if qualified by training or experience, or after full disclosure to their employers or clients of pertinent qualifications;
d. Maintain their professional skills at the level of the state of the art, and recognize the importance of currents events in their work;
e. Advance the integrity and prestige of the profession by practicing in a dignified manner and for adequate compensation.

Article II. Members shall, in their work:
a. Treat fairly all colleagues and co-workers, regardless of race, sex, age or national origin;
b. Report, publish and disseminate freely information to others, subject to legal and proprietary restraints;
c. Encourage colleagues and co-workers to act in accord with this Code and support them when they do so;
d. Seek, accept, and other honest criticism of work, and properly credit the contributions of others;
e. Support and participate in the activities of their professional societies;
f. Assist colleagues and co-worker in their professional development.

Article III. Members shall, in their relations with employers and clients:
a. Act as faithful agents or trustees for their employers or clients in professional and business matters, provided such actions conform with other parts of his Code;
b. Keep information on business affairs or technical processes of an employer or client in confidence while employed, and later, until such information's is properly released, provided that such actions conform with other parts of his Code;
c. Inform their employers, clients, professional societies or public agencies of which they are members or to which they make presentations, of any circumstance that could lead to a conflict of interest;
d. Neither give nor accept, directly or indirectly, any gift payment or service of more than nominal value to or from those having business relationships with their employers or clients;
e. Assist and advise their employers or clients in anticipating the possible consequences, direct or indirect, immediate or remote, of the projects, work or plans of which they have knowledge.

Article IV. Members shall, in fulfilling responsibilities to community:
a. Protect safety, health, and welfare of public and speak out against abuses in these areas affecting the public interest;
b. Contribute professional advice, as appropriate, to civic, charitable or other nonprofit organizations;
c. Seek to extend public knowledge and appreciation of the profession and its achievements.

IEEE Code of Ethics (von 1990)

(IEEE = Institute of Electrical and Electronics Engineers, gegründet 20er Jahre, ≈ 330000 Mitglieder)

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1 to accept responsibility in making engineering decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;

2 to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;

3 to be honest and realistic in stating claims or estimates based on available data;

4 to reject bribery in all its forms;

5 to improve the understanding of technology, its appropriate application, and potential consequences;

6 to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

7 to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;

8 to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;

9 to avoid injuring others, their property, reputation, or employment by false or malicious action;

10 to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

Approved by the IEEE Board of Directors

August 1990 (`http://www4.ncsu.edu/unity/users/j/jherkert/ethics.html`)

ISTE Ethical Code for Computer-Using Educators

(ISTE = International Society for Technology in Education; ≈ 12000 Mitglieder)

Principle I. Curriculum Issues— I have some responsibility for defining the roles of computers in the school curriculum and for assessing significant and likely intended and unintended consequences of those roles...

Principle II. Computer Access— I support and encourage policies that extend equitable computer access to all students, and I ill actively support well-reasoned programs and policies that promote such use...

Principle III. Privacy / Confidentiality— I have varying degrees of responsibility for the development of policy that guarantees the proper use of computerized and non-computerized information in the school's possession...

Principle IV. Teacher related Issues— ...In order to redefine the teacher's role in light of the integration of computers into classrooms, each teacher must have a minimum level of general computer literacy, including skills and knowledge about computers appropriate to the classroom setting and subject are. In addition, each teacher must accept the responsibility to practice as a professional according to the highest ethical standard...

Principle V. Student Issues— One way to measure success is by the progress of each student toward realization of potential as a worthy and effective citizen. To help fulfill this goal, I will:

a) help Students learn about future trends and possible impacts and consequences of a computerized society,
b) demonstrate respect for computer ethics in the school, which includes not permitting unauthorized duplication of software by my students,

c) insure that students have opportunities to evaluate their current and future roles and the impact their actions can have on future consequences in a computerized society,
d) help students to evaluate the models which underlie simulations on which major societal decisions are made, and
e) help students examine issues that relate to computer ethics.

Principle VI. Community Issues— The general community, parents and educators share responsibility for creating learning environments. In fulfilling responsibilities to the community I will:
a) provide training to the members of the educational or general community when asked and when practical to increase parental and community knowledge of possible educational goals that involve computers..., encourage parental involvement in long-term planning of computer use, coordinate expectations for computer use between home and school,
b) extend the standards for respect of copyright into school / community interactions, and
c) evaluate what control donors should have over the use of hardware and software they provide.

Principle VII. School Organization Issues— Effective and efficient use of computer in education requires organizational support.

Principle VIII. Software Issues— I have some responsibility for the acquisition, development and dissemination of software in the school environment...

Principle IX. Hardware Issues— I share responsibility for there quality and improvement of hardware used by educators and students...

Inhaltsangaben von weiteren Kodizes in Stichworten

(zusammengestellt von Dominik Schoop)

CPSR/PI Code of Fair Informations Practices

(CPSR = Computer Professionals for Social Responsibility; PI = Privacy International)

Datenmißbrauch stoppen
zu einem Zweck aufgenommene Daten sollen nicht ohne Zustimmung zu einem anderen Zweck benutzt werden.

Datenreduktion fördern
Nur Daten für einen bestimmten Zweck sammeln. Möglichst die Information nicht personenbezogen halten.

Datenintegrität fördern
Die Korrektheit, Zuverlässigkeit, Vollständigkeit und Zeitlosigkeit persönlicher Daten sicherstellen

Erlaubte Datenkontrolle
Benachrichtigte Subjekte der Datensätze über Datensatzhaltungspraktiken und Datengebrauch.
Erlaubte Einzelpersonen persönliche Informationen zu kontrollieren und zu korrigieren. Schaffe keine Systeme, die geheim Daten speichern.

Bilde eine Politik zur Vertraulichkeit
Schaffe und fördere eine Politik zur Vertraulichkeit von Informationen. Mache Politik öffentlich zugänglich.

Draft IFIP Code of Ethics

(IFIP = International Federation for Information Processing, gegr. 1960, eingebunden in die Struktur der UNESCO; IFIP ist der Dachverband der nationalen Informatikgesellschaften wie ACM, GI, etc.)

1. ethische Regeln für den einzelnen Fachmann:
    - soziale Verantwortung
        - menschliches Wohlergehen
        - Lebensqualität
        - soziale Konsequenzen der IT
    - Schutz der Privatsphäre (Vertraulichkeit)
        - Integrität und Privatsphäre achten
        - IT kann Bedrohung der Privatsphäre sein
    - persönliche Integrität
        - persönliche Integrität erhalten
        - kein Mißbrauch
    - fachliche Kompetenz
        - Kompetenz erhalten und verbessern
        - Verstehen der Grenzen des Sachverstands
    - persönliche Verantwortlichkeit
        - persönliche Verantwortung für Stellung und Arbeit
        - Aufgabe nur übernehmen, wenn Erfolg absehbar ist
        - Mitarbeiter über Arbeit informieren
        - IT-Systeme objektiv testen auf Effektivität für nicht schadende Anwendungen

2. ethische Regeln für internationale Organisationen
    - hohe Durchführungsstandards
        - Internationale Organisationen haben soziale Verantwortung
        - qualitativ gute Güter und Dienste anbieten
        - Zuverlässigkeit von Systemen wichtig
    - internationale Standards und Regulationen
        - internationale IT-Org. fördern den Fortschritt durch Schaffung von annehmbaren IT-Standards
        - multinationale Organisationen sind sich bewußt, dass nützliche internationale Informationsdienste den Einsatz aller erfordern
    - internationale rechtlicher Schutz
        - internationale IT-Organisationen brauchen rechtlichen Schutz
    - Produktivität und Qualität des Arbeitslebens eines Arbeitnehmers
        - Qualität des Arbeitslebens eines Angestellten fördern
        - dadurch steigt die Produktivität aber auch physische Sicherheit, persönliche Würde, menschliche Erfüllung
    - Anwenderbeteiligung und Feedback
        - Anwender / Benutzer (User) ist integrales Bestandteil eines IS, zu seinem Nutzen oder Schaden

Angelegenheiten des Users bei Entwicklung direkt einbeziehen

3. ethische Regeln für eine internationale rechtliche Informatik:
    Geistige Güter als Eigentum
        Ergebnisse von Kreativität bedürfen eines rechtlichen Schutzes
        (Hardware, Software, Telekommunikation, verwandte Güter und Dienste)
    internationales allgemeines Recht
    internationales Fernmelderecht
    internationales Strafrecht

4. ethische regeln für die öffentliche Politik
    Kommunikationsfreiheit
    Privatsphäre und Würde von Einzelpersonen
    humane Informationssysteme
    internationale Fähigkeit im Umgang mit Computern
    faire Möglichkeiten für Informationsdienste
    kulturelle Lebensqualität

Ingenieur An Engeneer's Hippocratic Oath

sich dem Dienste de Menschheit widmen
den Lehren den zustehenden Respekt entgegenbringen
loyal (treu) gegenüber dem Berufsstand handeln
aufrecht das Leben führen
Einsatz zum Wohle der Menschheit
enthalten von Korruption
Ausübung des Berufs nur zum Wohle der Menschlichkeit
keine kriminelle Handlungen
gegen Schlechtes und Ungerechtigkeit sich aussprechen
Gleichbehandlung
fachliches Wissen nicht gegen die Gesetze der Menschlichkeit einsetzen
Abfall vermeiden und nicht-erneuerbare Ressourcen schonen

Joel Rothstein Wolfson A Code of Professional Responsibility

Kritik an Kodizes, die fordern Interessenkonflikte zu vermeiden, aber nicht klären, was Interessenkonflikte sind.

Prinzip 1: Anwender nicht schädigen mit Absicht oder durch Interessenkonflikt
DR-1.1 kein Kodex, dem ein vernünftiger Anwender widersprechen muss
    kein Programm, gegen dessen Funktion ein vernünftiger Anwender Einwände haben würde
DR-1.2 keine wesentlichen falschen Angaben machen
DR-1.3 kein Informationsmißbrauch
DR-1.4 keinen Computer benutzen, um private Informationen zu erlangen
DR-1.5 Offenlegung einer möglichen Bestechung
DR-1.6 Fachmann in Projekt, das Tod oder Körperverletzung hervorrufen kann, muss sich

versichern, dass da Computersystem
- a) ordentlich geplant ist;
- b) von Fachleuten erstellt wurde;
- c) ohne Nachlässigkeit entwickelt wurde;
- d) adäquat getestet wurde;
- e) ordentlich installiert ist und gewartet wird.

Prinzip 2: keinen Schaden für Computer oder Fachleute verursachen

DR-2.1 Kopierrechte, Markenzeichen und Patentrechte nicht verletzen

DR-2.2 nur im zugegebenen Rahmen Nutzen ziehen

Prinzip 3: Leuten in Forschung und Entwicklung keinen Schaden zufügen

DR-3.1 Autorenschaft zugestehen

Prinzip 4: wahrheitsgemäß sich selber darstellen

DR-4.1. keine falsche Aussage machen über eine Computeranwendung oder -untersuchung

Prinzip 5: Kompetenz erhalten

DR-5.1 a) kompetent sein
- b) Kompetenz erarbeiten oder
- c) sich mit einem Kompetenten verbinden

DR-5.2 Mitgliedschaft in einer Gesellschaft zeigt nicht Kompetenz

DR-5.3 Kompetenz erhalten durch ständige Fortbildung

Prinzip 6: Ansehen des Berufsstandes fördern

DR-6.1 Verletzung des Kodex nicht unterstützen

DR-6.2. für Computergesellschaft nur mit Erlaubnis handeln

DR-6.3. Ungeschicklichkeit vermeiden

DR-6.4 fachliche und soziale Verantwortung übernehmen

Material zu Verantwortung der InformatikerInnen

Return-Path: <fiff-l-request@dia.informatik.uni-stuttgart.de> Received: from ifi.informatik.uni-stuttgart.de by tcs.inf.tu-dresden.de (4.1/SMI-4.1)
id AA14646; Mon, 24 Apr 95 18:56:20 +0200 Received: from dia.informatik.uni-stuttgart.de by ifi.informatik.uni-stuttgart.de with SMTP; Mon, 24 Apr 95 18:45:30 +0200 Received: by dia.informatik.uni-stuttgart.de; Mon, 24 Apr 1995 18:46:19 +0200 Received: by dia.informatik.uni-stuttgart.de with SMTP; Mon, 24 Apr 1995 18:46:03 +0200 Received: by fhg.de (mail-gw.fhg.de) with PRESMTP; Mon, 24 Apr 95 18:44:50 +0200 from FHG-GATEWAY Received: by fhg.de (mail-gw.fhg.de) with SMTP; Mon, 24 Apr 95 18:02:31 +0200 from iitb.iitb.fhg.de Rec-Date: Mon, 24 Apr 95 18:00:59 +0200
Received: by iitb.fhg.de; Mon, 24 Apr 95 18:01:53 +0200 Received: by vsk.iitb.fhg.de; Mon, 24 Apr 95 18:01:45 +0200 Received: by alice.iitb.fhg.de (4.1/SMI-4.1)
id AA00644; Mon, 24 Apr 95 18:00:59 +0200 Date: Mon, 24 Apr 95 18:00:59 +0200
From: hd@iitb.fhg.de (Wolfgang Hinderer) Message-Id: <9504241600.AA00644@alice.iitb.fhg.de> To: fiff-l@dia.informatik.uni-stuttgart.de Subject: Mangelt es der Informatik an Seriosität?

Wer ist mit mir der Ansicht, dass es der gegenwärtigen Informatik an Seriosität mangelt?

Vorweg: Dies ist keine Polemik gegen einzelne Personen, die möglicherweise Verantwortung für das Wohlergehen der Informatik tragen, sondern vielmehr Ausdruck einer sich mir aufdrängenden Befindlichkeit einer ganzen Disziplin.

Nun, nach dem allmählichen Ausklingen der Wirtschaftskrise wäre es eigentlich für den von dieser Krise hauptsächlich betroffenen Bereich, nämlich die Computerindustrie, -technik und -wissenschaft, an der Zeit, zu reflektieren, was da so über sie gekommen ist und warum wohl es die Informatik diesmal besonders hart getroffen hat.

Ich bin der Meinung, dass die Informatik selbst die Schuld daran trägt. Die klassischen Ingenieurwissenschaften vom Maschinenbau bis zur Elektrotechnik haben, da sie ja um ca. 100 Jahre älter sind, eine solide Grundlage, was die Gegenstandsbereiche, Methodiken und Denkvoraussetzungen angeht. Der Informatik kann niemand vorwerfen, dass sie diese Grundlagen noch nicht hat. Aber man kann von einer so jungen Ingenieursdisziplin verlangen, dass sie sich entsprechend verhält. Markige Reden und marktschreierische Methoden, gerade auch in der augenblicklichen Diskussion um Standort und internationale Konkurrenzfähigkeit, sind in keiner anderen Ingenieurwissenschaft so alltäglich wie in der Informatik.

Auf der anderen Seite steht das offensichtliche Unvermögen der heutigen Informatik, klare Bedingungen für das einwandfreie Funktionieren der gebauten Informatik-Systeme auch nur zu formulieren, geschweige denn zu realisieren. Auch jüngste Pannen wie die Gepäckanlage im Flughafen Denver, die Gleisstellwerkanlage in Hamburg-Altona oder ungeklärte Airbus-Abstürze führen nur zu gegenseitigen Schuldzuweisungen ohne sichtbare Betroffenheit oder das Eingeständnis, dass das für andere Ingenieursdisziplinen Selbstverständliche für die Informatik nicht erreichbar ist. Die vergangene Krise scheint mir eine Quittung für dieses laute Verhalten der Informatik zu sein, weil sich die Investoren und Nutzer allmählich verschaukelt fühlen.

Unsere heutigen Informatiksysteme sind so archaisch wie es das Auto der 20er Jahre war. Und es scheint so, als ob die Informatik sich anheischig machen wollte, mit diesen Autos den Strassenverkehr der 90er Jahre zu bewältigen. Wie sicherlich auch allen anderen Menschen, die intensiv mit Computerwerkzeugen arbeiten, passiert es mir im Schnitt jeden Tag mehr als einmal, dass beim

Umgang mit diesen Werkzeugen irgend ein Effekt auftritt, der erstens nicht auftreten dürfte und der mir zweitens noch nicht begegnet ist. - Das ist doch so, als ob keine Autofahrt ohne Panne verliefe!

Selbst - oder gerade - Fachleute verlieren zunehmend das Gefühl, ihre Computer-Werkzeuge wirklich zu beherrschen, im Gegensatz zu früher, als die Systeme und ihre Wechselwirkungen untereinander noch wesentlich weniger komplex waren und und nicht in dem Masse "ein unbekanntes Wesen" an den Tag legten. Gewiß könnte die Zunahme der Komplexität als Erklärung und Entschuldigung, gelten. Aber das Schlimme ist ja, dass man mit dem Problem einfach so lebt: Die Jungen, weil sie es nicht anders kennen und zunächst natürlich von den Möglichkeiten fasziniert sind, die Alten, weil es sie beim Gerangel um Marktsegmente stören würde, wenn sie sich auf die Komplexitätsprobleme einließen.

Ich sehe einige fachliche Gründe für die gegenwärtige Misere:

* Im Augenblick ist Theoriefeindlichkeit Mode, vermutlich gerade *weil* eine grundlegende Theorie der Informatik derzeit nicht existiert. Es wird statt dessen versucht, mit noch mehr Maschinenpower und immer neuen, umfangreicheren Tools die alten, niemals behobenen Konstruktionsfehler zuzukleistern. Schon seit langem sind keine wirklich grundlegenden theoretischen Ergebnisse mehr in die ingenieurwissenschaftliche Praxis der Informatik eingeflossen.

* Die Informatik kennt ihren Standort noch gar nicht. Ist sie ein Bestandteil der Physik? - Oder genauer: Sind ihre wissenschaftlichen Grundlagen Bestandteil der Physik?

Ich vertrete den Standpunkt: Ja. Und zwar ein Bestandteil, den es in der Physik bis jetzt noch nicht gibt, der aber methodisch dort ebenso hin gehört wie etwa die Thermodynamik. Man könnte diese neue Teildisziplin vielleicht "Symbolik" oder "Physik der Organisation" nennen. Der physikalische "Mechanismus" der Sprache steht dabei jedenfalls im Mittelpunkt.

Sprache ist auf elementarer Ebene ein physikalischer Effekt wie andere Effekte auch. Und es wäre nur natürlich, wenn die Ingenieurskonstruktionen der Zukunft den Sprach-Anteil eben so innig vermischt mit den übrigen in den Bauwerken verwirklichten Konzepten enthielten, wie das heute schon für alle mechanischen, elektrischen und sonstigen Konzepte eine Selbstverständlichkeit ist. Der Schock, den die Entwicklung der Werkzeuge des Menschen im Moment durchmacht, kann wohl in Analogie gesehen werden zu dem Schock in der biologischen Evolution durch die Entwicklung des sprachfähigen Menschen aus dem Tierreich.

* Das Verständnis der Informatik als Gestaltungswissenschaft, wie es in einigen Aufsätzen des von W. Coy et al. herausgegebenen Bandes "Sichtweisen der Informatik" (Vieweg, 1992) vertreten wird, führt bezüglich der Grundlagenfindung m.E. in die Irre. Die Entwicklung einer gestaltungswissenschaftlichen Tradition der Informatik ist sicher sehr wichtig, gerade auch im Hinblick auf die Ethischen Leitlinien der Gesellschaft für Informatik und das Verständnis der Informatik als Ingenieurwissenschaft mit weitreichenden sozialen Folgen. Aber eine solche Tradition kann erst auf einer soliden naturwissenschaftlichen Begründung der Informatik aufbauen, sie kann diese Grundlage keinesfalls liefern.

Erst wenn die physikalischen Prinzipien von Organisation, so wie sie in jeglicher Informatik inhärent vorhanden ist, in einer naturwissenschaftlichen Weise eingeordnet sind und Methodiken existieren, die darauf aufbauen, kann m.E. eine neue seriöse Ära der Informatik beginnen. Deshalb meine ich, dass es der Informatik gegenwärtig gut täte, sich in Punkto Herstellen von Zuverlässigkeit und Belastbarkeit der Informatik-Systeme einstweilen von anderen physikalischen und ingenieurwissenschaftlichen Teildisziplinen an die Hand nehmen zu lassen.

Ich könnte mir vorstellen, dass sich innerhalb des Forums FIFF ein Forum zur Diskussion der hier angesprochenen Kritik auftut. Eine selbstkritische Bestandsaufnahme in voller Loyalität zu "unserem" Fach täte, so hoffe ich, dieser Disziplin wohl.

W. Hinderer

Dipl.-Math. Wolfgang Hinderer
Fraunhofer-Institut für Informations- und Datenverarbeitung – IITB
Fraunhoferstraße 1
D-76131 Karlsruhe, Germany

e-mail: hd@iitb.fhg.de
Fon: 0721-6091-299
Fax: 0721-6091-413

Return-Path: <fiff-l-request@dia.informatik.uni-stuttgart.de> Received: from ifi.informatik.uni-stuttgart.de by tcs.inf.tu-dresden.de (4.1/SMI-4.1)
id AA15215; Tue, 25 Apr 95 11:37:19 +0200 Received: from dia.informatik.uni-stuttgart.de by ifi.informatik.uni-stuttgart.de with SMTP; Tue, 25 Apr 95 11:29:10 +0200 Received: by dia.informatik.uni-stuttgart.de; Tue, 25 Apr 1995 11:29:53 +0200 Message-Id: <199504250929.LAA16527@dia.informatik.uni-stuttgart.de> Received: by dia.informatik.uni-stuttgart.de with SMTP; Tue, 25 Apr 1995 11:29:51 +0200 Received: by merian.iig.uni-freiburg.de (1.37.109.4/16.2) id AA14328; Tue, 25 Apr 95 11:30:44 +0200 From: Frieder Strauss <frieder@modell.iig.uni-freiburg.de> Subject: Re: Mangelt es der Informatik an Seriosität? To: hd@iitb.fhg.de
Date: Tue, 25 Apr 95 11:30:44 MESZ
Cc: fiff-l@dia.informatik.uni-stuttgart.de In-Reply-To: <9504241600.AA00644@alice.iitb.fhg.de>; from "Wolfgang Hinderer" at Apr 24, 95 6:00 pm Mailer: Elm [revision: 70.85]

Wolfgang Hinderer (hd@iitb.fhg.de) schrieb unter anderem

>Wer ist mit mir der Ansicht, dass es der gegenwärtigen Informatik an Seriosität mangelt?
>...

>* Das Verständnis der Informatik als Gestaltungswissenschaft, wie es in einigen Aufsätzen des von W. Coy et al. herausgegebenen Bandes "Sichtweisen der Informatik" (Vieweg, 1992) vertreten wird, führt bezüglich der Grundlagenfindung m.E. in die Irre. Die Entwicklung einer gestaltungswissenschaftlichen Tradition der Informatik ist sicher sehr wichtig, gerade auch im Hinblick auf die Ethischen Leitlinien der Gesellschaft für Informatik und das Verständnis der Informatik als Ingenieurwissenschaft mit weitreichenden sozialen Folgen. Aber eine solche Tradition kann erst auf einer soliden naturwissenschaftlichen Begründung der Informatik aufbauen, sie kann diese Grundlage keinesfalls liefern.

Ohne hier direkt eine Pro oder Contra- Argumentation für die "Sichtweisen der Informatik" vertreten zu wollen:

Gestaltung fängt doch da an, wo eine `Konstruktions'-Entscheidung NICHT durch softwaretechnische, theoretische, .. Randbedingungen festgelegt ist. Die Einbeziehung der Organisation, ergonomische Fragen, eine menschengerechte Arbeit(1) könnte doch auch in die Gestaltung einfließen, oder hälst Du das für unwichtig? Das sind aber gerade Aspekte, die bei einer naturwissenschaftlichen Begründung der Informatik nicht automatisch einfließen.

(1) Soll eine Software vorgangsbasiert wie bei der Fließbandarbeit bedient werden, schneller zu lernen aber auch langweilig? oder soll der Mensch selber entscheiden können und dafür dann aber auch qualifiziert werden.

Auch wenn wir noch keine Theorie der Informatik haben (ob die primär naturwissenschaftlich begründet sein wird?), ist die Frage, ob, was und wieviel wir als Informatiker gestalten können doch sehr zentral. Ich will zumindestens auch nicht bei der Softwarekonstruktion die gesamten Orga-Probleme einer Firma lösen müssen, weil die das selber nicht auf die Reihe bekommen -- das kann ich nämlich nicht.

ok das war ein erster Schnellschuß als Antwort, in der Hoffnung auf eine weitere Diskussion

Frieder Strauss

OFFICE: Institut für Informatik und Gesellschaft
A.-L.-Universität Freiburg, Friedrichstr. 50
D-79098 Freiburg, p. +761-203-4954
Private: Egertenstr. 2, D-79115 Freiburg, p. +761-491167
e-mail: frieder@modell.iig.uni-freiburg.de http: //www.iig.uni-freiburg.de/modell/users/frieder/

Return-Path: <fiff-l-request@dia.informatik.uni-stuttgart.de> Received: from ifi.informatik.uni-stuttgart.de by tcs.inf.tu-dresden.de (4.1/SMI-4.1)
id AA16602; Tue, 25 Apr 95 14:54:01 +0200 Received: from dia.informatik.uni-stuttgart.de by ifi.informatik.uni-stuttgart.de with SMTP; Tue, 25 Apr 95 14:33:43 +0200 Received: by dia.informatik.uni-stuttgart.de; Tue, 25 Apr 1995 14:34:36 +0200 Received: by dia.informatik.uni-stuttgart.de with SMTP; Tue, 25 Apr 1995 14:34:24 +0200 Received: by fhg.de (mail-gw.fhg.de) with PRESMTP; Tue, 25 Apr 95 14:33:07 +0200 from FHG-GATEWAY Received: by fhg.de (mail-gw.fhg.de) with SMTP; Tue, 25 Apr 95 14:33:03 +0200 from iitb.iitb.fhg.de Rec-Date: Tue, 25 Apr 95 14:32:52 +0200
Received: by iitb.fhg.de; Tue, 25 Apr 95 14:33:06 +0200 Received: by vsk.iitb.fhg.de; Tue, 25 Apr 95 14:32:58 +0200 Received: by alice.iitb.fhg.de (4.1/SMI-4.1)
id AA00949; Tue, 25 Apr 95 14:32:52 +0200 Date: Tue, 25 Apr 95 14:32:52 +0200
From: hd@iitb.fhg.de (Wolfgang Hinderer) Message-Id: <9504251232.AA00949@alice.iitb.fhg.de> To: frieder@modell.iig.uni-freiburg.de
Subject: Re: Mangelt es der Informatik an Seriosität? Cc: fiff-l@dia.informatik.uni-stuttgart.de

Frieder Strauss (frieder@modell.iig.uni-freiburg.de) schreibt:

>Gestaltung fängt doch da an, wo eine `Konstruktions'-Entscheidung NICHT durch softwaretechnische, theoretische, .. Randbedingungen festgelegt ist. Die Einbeziehung der Organisation, ergonomische Fragen, eine menschengerechte Arbeit(1) könnte doch auch in die Gestaltung einfließen, oder hälst Du das für unwichtig? Das sind aber gerade Aspekte, die bei einer naturwissenschaftlichen Begründung der Informatik nicht automatisch einfließen.

>(1) Soll eine Software vorgangsbasiert wie bei der Fließbandarbeit bedient werden, schneller zu lernen aber auch langweilig? oder soll der Mensch selber entscheiden können und dafür dann aber auch qualifiziert werden.

Gestaltung in einer Ingenieurwissenschaft kann erst da anfangen, wo die grundlegenden Möglichkeiten des Handwerkszeugs beherrscht werden. Und da muss dann tatsächlich der Mensch im Zentrum stehen. Mir geht es aber, wie ich hoffe, deutlich gemacht zu haben, gerade um jenes Handwerkszeug, dessen Möglichkeiten nicht Randbedingung, sondern Grundlage sind. Erst darauf aufbauend - und nicht `dagegen' - kann (Entwurfs-) Freiheit entstehen. Dies gilt übrigens ebenso in anderen Disziplinen, z.B. der Automobil-Konstruktion.

>Auch wenn wir noch keine Theorie der Informatik haben (ob die primär naturwissenschaftlich begründet sein wird?), ist die Frage, ob, was und wieviel wir als Informatiker gestalten können doch sehr zentral. Ich will zumindestens auch nicht bei der Softwarekonstruktion die gesamten Orga-Probleme einer Firma lösen müssen, weil die das selber nicht auf die Reihe bekommen -- das kann ich nämlich nicht.

Methodisch haben die Orga-Probleme einer Firma einiges gemein mit den Orga-Problemen in einem Programmsystem (kein Wunder, dass sie nicht gelöst sind). Es kommt darauf an, dieses sehr wohl zu trennen von Methodiken des übergeordneten sozio-technischen und des eigentlich menschlichen Bereichs. Ich will nicht verkennen, dass die Informatik deutlicher als andere Ingenieurwissenschaften hier an einer Nahtstelle zwischen (exaktem) naturwissenschaftlichem Bereich und (menschzentriertem) geisteswissenschaftlichem Bereich liegt. Was aber naturwissenschaftlich geklärt werden kann - auch im Orga-Bereich -, das muss auch. Sonst gerät der gesamte darauf aufbauende menschzentrierte Bereich ins Schwimmen.

W. Hinderer

Dipl.-Math. Wolfgang Hinderer
Fraunhofer-Institut für Informations- und Datenverarbeitung – IITB
Fraunhoferstraße 1
D-76131 Karlsruhe, Germany

e-mail: hd@iitb.fhg.de
Fon: 0721-6091-299
Fax: 0721-6091-413