# „Datenschutz – mausetot?“

Martin Rost



## Gliederung

„Es geht nicht um Privatheit, sondern um die soziale Beherrschbarkeit der Maschinerie.“
(Wilhelm Steinmüller, Autor des 1. Datenschutzgutachtens von 1971)

1. Was meint „Datenschutz“?
2. Schutzziele und Standard-Datenschutzmodell
3. Schutzziele, Geltungsanforderungen und Menschenwürde

# Privatheit wird/ist Fiktion?

heise online > News > 2013 > KW 11 > Studie: Facebook-Klicks sagen Eigenschaften

11.03.2013 21:15 « Vorige | Nächs

**Studie: Facebook-Klicks sagen Eigenschaften voraus**

PRIVATSPHÄRE

**"Datenschutz droht sich als Fiktion zu erweisen"** ZEIT ONLINE

**Völkerkunde bei Facebook**

*23.01.13* – Tom Simonite

**Schlagwörter:** Big Data, Soziologie, Facebook

**Ein Team aus Sozialwissenschaftlern und Informatikern durchleuchtet bei Facebook die gewaltigen Mengen an persönlichen Daten. Wie wird das Unternehmen die Erkenntnisse über seine Nutzer verwenden? Technology Review hat sich mit den Forschern getroffen.**

**Google Glass app identifies you by your fashion sense**

› 07 March 2013 by Paul Marks
› Magazine issue 2907. Subscribe and save

CAN'T find a face in the crowd? Not to worry, a human recognition system can spot people for you – even when their faces aren't visible. Designed for Google's forthcoming Glass headset, it recognises people by the clothes they are wearing. Their name is then overlaid on the headset's video.

**Kreditwürdigkeit: Schufa will Facebook-Nutzer durchleuchten** SPIEGEL ONLINE

CNET › News › The Digital Home › Assange: Facebook is an 'appalling spy machine'

**Assange: Facebook is an 'appalling spy machine'**

Julian Assange, the head of WikiLeaks, also takes aim at Google and Yahoo in interview with a Russian news site, saying that they have "built-in interfaces for U.S. intelligence."

by Don Reisinger | May 3, 2011 9:45 AM PDT

04.05.2012 19:13 « Vorige | N

**Studie: Was soziale Netzwerke über Nicht-Mitglieder wissen**



# Was meint „Datenschutz“?

## Datenschutz

Datenschutz…

ist nicht nur das, was im **Datenschutzrecht** steht
(=> *juristischer Kurzschluss*).

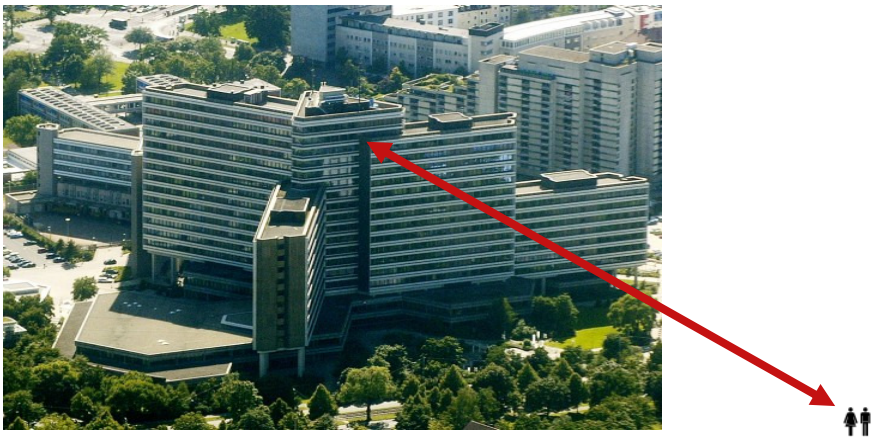
ist nicht mit **Datensicherheit** gleichzusetzen
(=> *technizistischer Kurzschluss*).

Aber: Was meint dann Datenschutz?



## Objektbereich des Datenschutzes

Datenschutz beobachtet die organisierte Informationsverarbeitung und Kommunikation in der *asymmetrischen Machtbeziehung* zwischen Organisationen und Personen.



## Objektbereich des Datenschutzes

Konkret sind das die *externen* Machtbeziehungen zwischen…

- öffentlicher Verwaltung und deren externen **Bürgern,**
- privaten Unternehmen und deren **Kunden,**
- IT-Infrastruktur-Providern und deren **Nutzern** / **Kunden** (bspw. Access-, Suchmaschinen-, Mail-, Socialnetwork-Betreiber);
- Praxen / Instituten / Gemeinschaften und deren **Patienten, Mandanten, Klienten;**
- Wissenschaftsorganisationen und deren Forschungsobjekten **Individuen, Subjekte, Menschen;**

sowie die *internen* Machtbeziehungen zwischen…

- Organisationen (Arbeitgeber, auch: Kirche, Militär, (Sport-)Verein) und deren **Mitarbeitern der Mitgliedern** (Schüler, Patienten, Gefangenen, Soldaten, …).



## Datenschutz und Datensicherheit

- Datenschutz setzt funktionierende Mechanismen der Datensicherheit voraus.
  Datensicherheit und Datenschutz stehen jedoch auch in einem systematischen **Spannungsverhältnis.**

- ***Datensicherheit:***
  **Grundsätzlich ist jede Person ein möglicher Angreifer einer Organisation!**
  (profesionelle Hacker, Script-Kiddies, Kunde, Konkurrent, (ehemalige) Mitarbeiter…)
  Die Folge? Die Person muss nachweisen, dass sie kein Angreifer ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss. Klassischer Schutz vor Personen: Authentisierung, Autorisierung der Person, Protokollierung, Intrusion-Detection.

- ***Datenschutz:***
  **Grundsätzlich ist jede Organisation ein möglicher Angreifer auf eine Person!**
  (Sicherheitsbehörden, Verwaltungen, Versicherungen, IT-Provider, SocialWeb-Provider…)
  Die Folge? Die Organisation muss (jederzeit) prüffähig nachweisen (können), dass sie kein Angreifer ist, sich an die Regeln hält und bei all dem ihre Verfahren und Prozesse beherrscht.

## Was ist zu tun…?

Als Kommunikations-Techniker würde man nun was genau machen?

Genau… man macht erst einmal alle Ports dicht!
Dann Anforderungen sichten, die erfüllt sein müssen, damit gewünschte Kommunikation möglich ist.

Also „Port 80“ und nen ssh-Port öffnen und in besonderen Fällen noch n Applicationlevel-Proxy davor. (Und vielleicht noch nen honeypot, büschen intrusion-detection, nagios usw. usw.)



## Kernregelungsstrategie des Datenschutzrechts

Grundsatz:

**Es dürfen keine personenbezogene Daten verarbeitet werden** PUNKT

**=> „Verbot mit Erlaubnisvorbehalt“<=**

Eine Ausnahme von diesem Grundsatz ist zulässig, wenn

- ein **Gesetz** die Verarbeitung regelt, was insbesondere für den öffentlichen Bereich gilt, oder wenn
- eine **Einwilligung** vorliegt, was inbesondere im privaten Bereich vorliegt, wobei an die Einwilligung Bedingungen geknüpft sind:
  - Bestimmung des Zwecks
  - Freiwilligkeit,
  - vollumfängliche Informiertheit und Bestimmtheit der Verarbeitung,
  - abschließende Bestimmung der Empfänger.

## Und was ist nun zu tun?

Nun sind neben den Technikern
die Organisatoren gefragt!

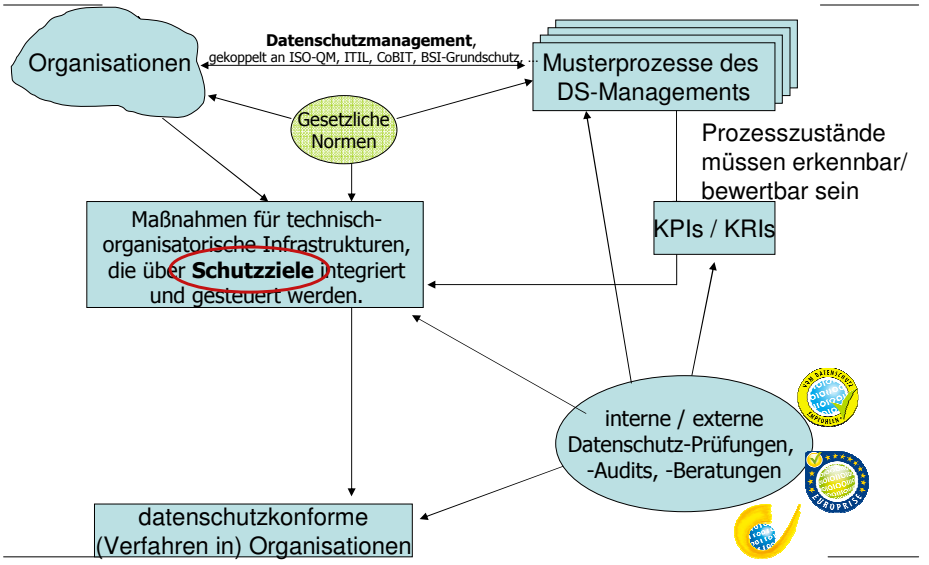
Wir brauchen Ziele, die alle verstehen:
Die Techniker, die Betriebswirte,
die Juristen, vor allem: das Management!

Und: Welche Ziele sind das?

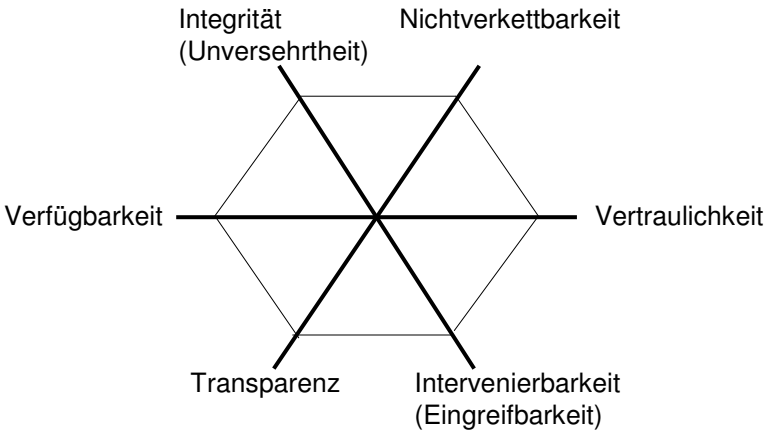


## Big Picture

### Prozesse, DS-Management, Schutzziele, KPI/KRI

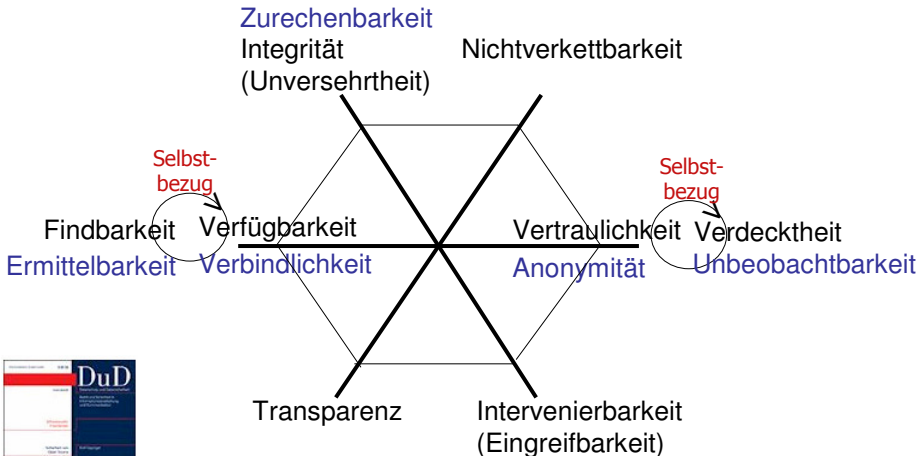


## Schutzziele als operativ-umsetzbare Anforderungen des Datenschutzes an Organisationen






## Schutzziele vollständig







Rost, Martin / Pfitzmann, Andreas, 2009:
Datenschutz-Schutzziele - revisited;
in: DuD - Datenschutz und Datensicherheit,
33. Jahrgang, Heft 6, Juli 2009: 353-358

Legende:
Informations-Inhalte
Informations-Umfeld

# Maßnahmen zur Umsetzung von Datenschutzzielen

- **Sicherstellung von *Verfügbarkeit***
  Daten/Prozesse: Redundanz, Schutz, Reparaturstrategien
- **Sicherstellung von *Integrität***
  Daten: Hash-Wert-Vergleiche
  Prozesse: Festlegen von Min./Max.-Referenzen, Steuerung der Regulation
- **Sicherstellung von *Vertraulichkeit***
  Daten: Verschlüsselung
  Prozesse: Rollentrennungen, Abschottung, Containern
- **Sicherstellen von *Transparenz* durch Prüffähigkeit**
  Daten: Protokollierung
  Prozesse: Dokumentation von Verfahren
- **Sicherstellen von *Nichtverkettbarkeit* durch Zweckbestimmung/-bindung**
  Daten: Pseudonymität, Anonymität (anonyme Credential)
  Prozesse: Identitymanagement, Anonymitätsinfrastruktur, Audit
- **Sicherstellen von *Intervenierbarkeit* durch installierte Ankerpunkte**
  Daten: Zugriff auf Betroffenen-Daten durch den Betroffenen
  Prozesse: SPOC für Änderungen, Korrekturen, Löschen, Aus-Schalter, Changemanagement,



| | Daten | Systeme | Prozesse |
|---|---|---|---|
| **Verfügbarkeit** | D1.1 Einschränkung von Lösch-/Veränderungsrechten<br>D 1.2 Schutz vor Schadsoftware<br>D 1.3 Backup der Daten | S 1.1: Schutz vor Schadsoftware<br>S 1.2: Backup von Konfigurationen und Software<br>S 1.3: Hardwareredundanz<br>S 1.4: Ausweichräume, und -Netze | P 1.1: Vertretungspersonal<br>P 1.2: Fähigkeit zur Aufgabenerledigung durch Dri<br>(Vorbereitung Outsourcing)<br>P 1.3: Ausweichprozesse, Amtshilfe |
| **Vertraulichkeit** | D 2.1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst)<br>D 2.2: Protokollierung lesender Zugriffe<br>D 2.3: Verschlüsselung der Daten<br>D 2.4: Ende-zu-Ende-Verschlüsselung | S 2.1: Einschränkung von lesenden Zugriffsrechten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways)<br>S 2.2: Verschlüsselung auf Systemebene (Festplatten, Datenbank) | P 2.1: Verpflichtung auf das Datengeheimnis (BDS<br>P 2.2: Verschwiegenheitsvereinbarungen<br>P 2.3: Geeignete Organisation bei der Vergabe von Zugriffsrechten („need-to-know“) |
| **Integrität** | D 3.1: Einschränkung von Schreib- und Änderungsrechten<br>D 3.2: Protokollierung von schreibenden/ändernden Zugriffen<br>D 3.3: Protokollierung geänderter Daten<br>D 3.4: Nachberichtigung<br>D 3.5: technische Integritätskontrollen (Signaturen/Hashes) | S 3.1: Einschränkung von schreibenden Zugriffen/Konfigurationmöglichkeiten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways)<br>S 3.2: Regelmäßige Integritätsprüfungen/Audits | P 3.1: Detaillierte Planung von Verfahren und Verfahrensschritten<br>P 3.2: Geordnete Zuweisung von Rechten und Roll<br>P 3.3: Geordnete Änderung von Verfahren und Verfahrensschritten<br>P 3.4: Regelmäßige Überprüfung |
| **Nicht-Verkettbarkeit** | D 4.1: Einschränkung von Verarbeitung-s-/Nutzungs- /Übermittlungsrechten für einzelne Daten<br>D 4.2: Kennzeichnung der Zwecke auf Ebene der Daten<br>D 4.3: Einschränkung von identifizierenden Daten; Pseudonymisierung<br>D 4.4: Anonymisierung von Daten | S 4.1: Kennzeichnung der Zwecke auf Ebene des Systeme<br>S 4.2: Trennung von Datenbeständen<br>S 4.3: Einschränkungen von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten (Funktionalitätseinschränkung)<br>S 4.4: Trennung auf Systemebene (Software, Hardware; Mandantenfähigkeit) | P 4.1: Trennung auf Verfahrensebene<br>P 4.2: Rechte + Rollenvergabe, ggf. an eine andere rechtliche Entität (z. B. Personalvertretung)<br>P 4.3: Gewaltenteilung |
| **Transparenz** | D 5.1: Dokumentation der Datenfelder einschließlich Erforderlichkeit<br>D 5.2: Protokollierung von Datenverarbeitungen mit Schutzbedarf zunehmender Detaillierungsgrad und Speicherdauer<br>D 5.3: Integritätsschutz der Protokolle (separater Protokollierungsserver) | S 5.1: Dokumentation der Systeme (Hardware, Software, Algorithmen)<br>S 5.2: Protokollierung von Konfigurationsänderungen<br>S 5.3: zunehmende Kontrolldichte bei höherem Schutzbedarfen; automatisiertes Monitoring | P 5.1: Dokumentation des Verfahren und einzelner Prozesse (einschließlich beteiligter Organisationsei Rollen und Übermittlungen an Dritte)<br>P 5.2: Dokumentation der Änderungsprozesse |
| **Intervenierbarkeit** | D 6.1: Schaffung notwendiger Datenfelder (z. B. für Gegendarstellungen) | S 6.1 Funktionalitäten in den Systemen für die Bearbeitung von Sperrungen, Widersprüchen, Beauskunftungen<br>S 6.2 Funktionalitäten in den Systemen für die Umsetzung von weiteren Rechten Betroffener (z. B. Rufnummerunterdrückung, Pseudonyme Nutzungsmöglichkeit, etc.)<br>S 6.3 Funktionalitäten für Betroffene, einzelne Betroffenenrechte direkt wahrzunehmen (z.B. Auskunftsportal, „Datenbrief“, Zusendung von Protokollen, eigene Änderungsmöglichkeiten)<br>S 6.4 Steuerungsmöglichkeiten für einzelne Funktionen („Overrride“) bei automatisierten Einzelentscheidungen<br>S 6.5 Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem | P 6.1: Organisation der Umsetzung der Betroffenen (Rechte + Rollen für Auskunft, Sperrungen)<br>P 6.2: Organisation der Umsetzung der Betroffenen (Rechte und Rollen bei der Bearbeitung von Gegendarstellungen und Einwänden; Übersteuer automatisierter Einzelfallentscheidungen)<br>P 6.3: Single Point of Contact für Datenschutzfrag |


„Thomas Probst: **Generische Schutzmaßnahmen für Datenschutz-Schutzziele**“; DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6, Juni 2012: 439-444

# Schutzziele

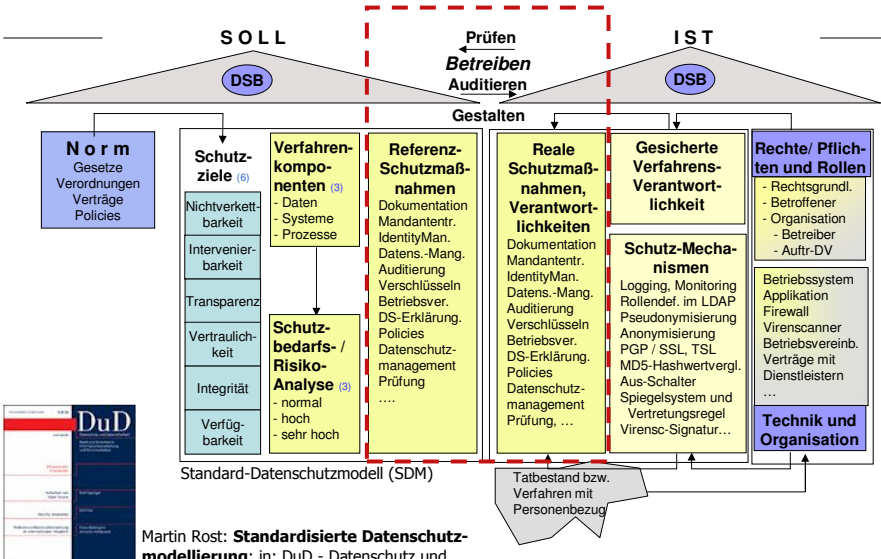
## im Gesetz (LDSG-SH, Januar 2012, §5)

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Sie müssen gewährleisten, dass

- Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können **(Verfügbarkeit),**
- Daten unversehrt, vollständig, zurechenbar und aktuell bleiben **(Integrität),**
- nur befugt auf Verfahren und Daten zugegriffen werden kann **(Vertraulichkeit)**,
- die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann **(Transparenz)**,
- personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können **(Nicht-Verkettbarkeit)** und
- Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 wirksam ermöglichen **(Intervenierbarkeit)**.



# Datenschutz: umsetzen und prüfen







Martin Rost: **Standardisierte Datenschutz-modellierung**; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438.

## Zum Schluss…

**zwei Anmerkungen zu**
**Technikneutralität und Würde**



## Grundrecht Datenschutz

**Artikel 1 Grundgesetz**

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

**Artikel 2 Grundgesetz**

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

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

# „Volkszählungsurteil“ des BVerfG. von 1983

Zentrale Datenschutz-Figur:
„Recht auf **informationelle Selbstbestimmung**“
**(BVerfGE 65, 1 - Volkszählung** (http://www.servat.unibe.ch/dfr/bv065001.html))

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

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



# **Geltungsansprüche** an eine vernünftige Rede

(nach Habermas 1980, http://de.wikipedia.org/wiki/Geltungsanspruch#Universalpragmatik)

Mit der Durchführung von Sprechakten werden „Geltungsansprüche“ verbunden. Ihre Erfüllung muss im kommunikativen Handeln von den Sprechern unterstellt werden. (…) Habermas unterscheidet vier Arten von Geltungsansprüchen sinnhafter Kommunikationen, die nicht aufeinander zurückgeführt werden können:

- ***Verständlichkeit***
  Der Sprecher unterstellt das Verständnis der gebrauchten Ausdrücke. Bei Unverständnis wird zur Explikation durch den Sprecher aufgefordert.
- ***Wahrheit***
  Bezüglich des propositionalen Gehalts der Sprechakte wird Wahrheit unterstellt. Wird diese bezweifelt, muss ein Diskurs klären, ob der Anspruch des Sprechers zurecht besteht.
- ***Richtigkeit***
  Die Richtigkeit der Norm, die mit dem Sprechakt erfüllt wird, muss anerkannt werden. Auch dieser Geltungsanspruch ist nur diskursiv einlösbar.
- ***Wahrhaftigkeit***
  Die Sprecher unterstellen sich gegenseitig Wahrhaftigkeit (Aufrichtigkeit). Erweist sich diese Antizipation (Voraussetzung) als unhaltbar, kann der Hintergrundkonsens nicht mit dem unwahrhaften Sprecher selber wiederhergestellt werden.

## Folgerungen für Gestaltung von IKT in einer modernen Gesellschaft

1. Die Umsetzung der sechs elementaren Schutzziele des Datenschutzes ist eine Voraussetzung dafür, dass die Geltungsanforderungen an eine vernünftige Rede in einer technisch vermittelten Kommunikation (Telefon, Internetdienste) in einer modernen Gesellschaft zur Geltung kommen können. Das heisst: **Kommuniktions- und Informationstechnik muss neutral funktionieren und darf niemanden strukturell bevorteilen**.

2. Wenn die Definition von Menschenwürde nicht mehr christlich angebunden wird (wie noch im GG-Kommentar Dürig/Maunz bis 2003), sondern als „immer auch kommunikativ eingebettet“ begriffen wird, **dann erzeugt eine unfaire und unbeherrschte I&K-Technik strukturelle Risiken für die Würde des Menschen.**



Vielen Dank für Ihre Aufmerksamkeit!

Martin Rost
martin-rost@web.de
http://www.maroki.de