Zur Soziologie des Datenschutzes

Martin Rost

Seminar, Dresden
29.04.2013

Ziel: Verständnis für zwei Thesen erzeugen

- These 1: *Soziologische Fassung von Datenschutz*
  Datenschutz ist die Beobachtung der Differenz von Organisation und Funktionssystem in der Form „Person“.
- These 2: *Soziologische Begründung der Schutzziele des Datenschutzes*
  Die Schutzziele des Datenschutzes sind „vernünftigerweise geltende Ansprüche an das Operieren technisch-organisatorischer Systeme bzw. gesellschaftlicher Infrastrukturen“.

Gliederung

- **Was meint Datenschutz?**
  1. *Objekt*: Asymmetrische Organisations-Personen-Verhältnisse
  2. *Kernregelung des Datenschutz-Rechts*: Verbot mit Erlaubnisvorbehalt
  3. *Datenschutzrecht*: EU, BDSG, LDSG, Spezialgesetze
  4. *Akteure*: Datenschutzbeauftragte (BfDI, LfD, DSB)
  5. *Schutzziele:* Integration von Recht, Technik, Organisation über Schutzziele
  6. Beispiele für *technisch-organisatorische Maßnahmen*: Protokollierung, Dokumentation, Identitätenmanagement
  7. *Modellierung* von Datenschutz-Aktivitäten
  8. *Facebook* im Lichte der Schutzziele und des Standard-Datenschutzmodells
- **Was meint Soziologie?**
  1. 3-Welten-Theorie, das Gesellschaftliche als „*Realität sui generis*“ (Durkheim)
  2. *Kommunikatives Handeln* (Habermas)
     Handeln und Sprechen als praktische Aktivitäten
  3. *Funktionale Systemtheorie* (Luhmann)
     Interaktion, Organisation und funktional-differenzierte Gesellschaft
  4. *Facebook* im Lichte der Soziologie
- **Gesellschaftliche Funktion des Datenschutzes**
  DS deckt Strukturdefekte auf; Schutzziele umzusetzen ist vernünftig; die „Würde des Menschen“ wird kommunikativ konstituiert, deshalb Anford. an Komm-Technik

Was ist und was macht Datenschutz?

Privatheit wird/ist nur noch 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 interfaces for U.S. intelligence."

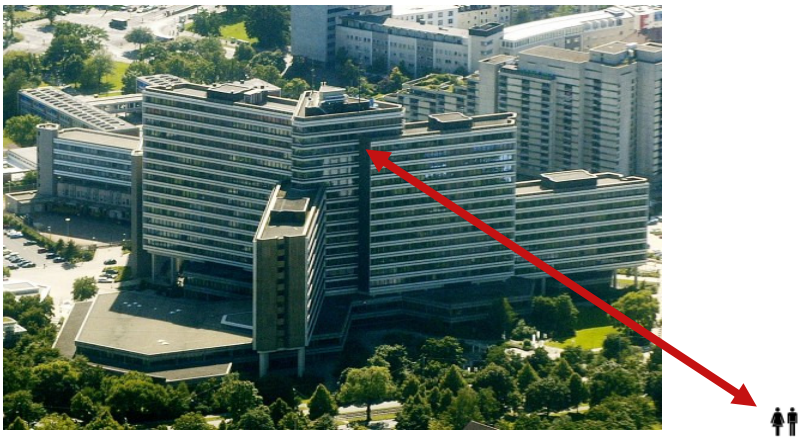
by Don Reisinger | May 3, 2011 9:45 AM PDT

04.05.2012 19:13 « Vorige | N

Studie: Was soziale Netzwerke über Nicht-Mitglieder wissen

Objektbereich des Datenschutzes

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



Objektbereich des Datenschutzes

- **Datenschutz beobachtet** die organisierte Informationsverarbeitung und Kommunikation in der *asymmetrischen Machtbeziehung* zwischen Organisationen und Personen. Konkret umfasst das vor allem die Beziehung zwischen:
  - öffentlicher Verwaltung und deren **Bürgern;**
  - privaten Unternehmen und deren **Kunden;**
  - Praxen / Instituten / Gemeinschaften und deren **Patienten, Mandanten, Klienten;**
  - Wissenschaftsorganisationen und deren Forschungsobjekten **Individuen, Subjekte, Menschen;**
  - IT- und Energie-Infrastruktur-Providern und deren **Nutzern** (bspw. Access-, Suchmaschinen-, Mail-, Socialnetwork-Betreiber, Energie-Unternehmen, …);
  - Institutionen und deren **Mitarbeitern oder Mitgliedern.**
- **Datenschutz bewertet** die asymmetrischen Machtbeziehungen zwischen strukturell mächtigen Organisationen und deren Klientel im Hinblick darauf, ob diese aus Sicht der Personen *unter Bedingungen gestellt* sind.

1. Zwischenfazit

- **Datenschutz:**
  Jede Organisation ist ein Angreifer!
- Datensicherheit:
  Jede Person ist ein Angreifer!

Datenschutzrecht, abgeleitet aus Art. 1, 2 GG

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

(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.

Datenschutz „informationelle Selbstbestimmung“

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.

Was ist technisch zu tun?

Als Kommunikations-Techniker würde man nun was genau machen, um Personen gemäß Datenschutzrecht zu schützen?

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.

Datenschutz-Recht: Grundsätze

- **Bundesdatenschutzgesetz** (*BDSG*) erstreckt sich auf Privatpersonen, Bundesbehörden und Telekommunikationswirtschaft
- **Landesdatenschutzgesetze** erstrecken sich auf öffentliche Verwaltung eines Bundeslandes und Kommunen sowie Privatunternehmen (speziell in SH: DS-Verordnung)
- **EU:**
  - **Europäische Grundrechte-Charta**
  - **Datenschutz-Richtlinie** Wirkung über Import in deutsche Gesetze
- **Spezialgesetze**:
  - Telemedien-Gesetz, T-Kommunik-Gesetz, SGB, AO, LandesMeldeGes, LVerwGesetz/ PolizeiGes, PassGes, PersonalausweisGes, EnWG, AufenthaltsGes.

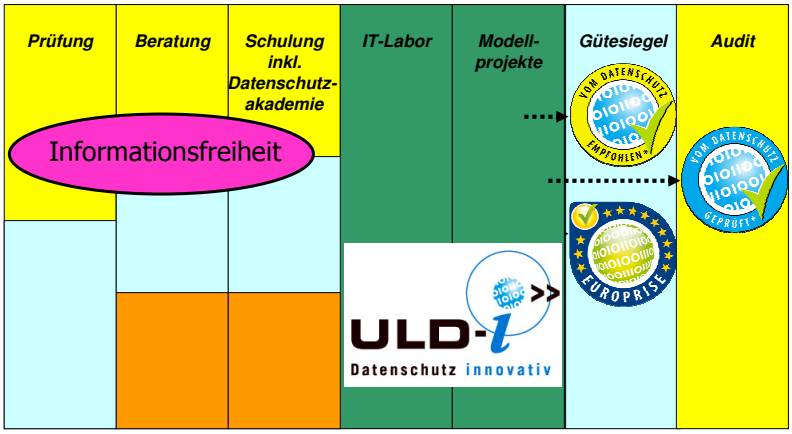
→ Regel: Die Spezialgesetze gehen den Allgemeingesetzen vor. ←

- Rechtmäßigkeit der Datenverarbeitung
  - Gesetzliche Rechtsgrundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeit
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Vorratsammlung
  - Verbot der automatisierten Einzelentscheidung
- Nutzung anonymisierter oder pseudonymisierter Daten

Datenschutzbeauftragte

- Die Aufgaben des **Bundesbeauftragten** für den Datenschutz und Informationsfreiheit (BfDI) sind in §4f, 4g BDSG geregelt. Der Zuständigkeitsbereich umfasst Behörden des Bundes und Unternehmen der Telekommunikationsunternehmen.
- Jedes Bundesland hat eigene **Landesdatenschutzbeauftragte** (LfD) gemäß landeseigenen gesetzlichen Grundlagen. Der Zuständigkeitsbereich umfasst die landeseigenen Behörden sowie Unternehmen mit Sitz im Bundesland. Einige LfDe sind auch zuständig für Vollzug des Informationsfreiheitsgesetzes (IfG).
- Wenn Organisationen personenbezogene Daten (Arbeitnehmerdaten, Kundendaten, Bürger) automatisiert verarbeiten, müssen in der Regel **behördliche** oder **betriebliche Datenschutzbeauftragte** bestellt werden.
- Der **Europäische Datenschutzbeauftragte** (EDSB) ist eine unabhängige Kontrollbehörde, die die Verarbeitung personenbezogener Daten bei den Organen und Einrichtungen der EU kontrolliert (Verordnung (EG) Nr. 45/2001 des europäischen Parlaments und Rates vom 18. Dezember 2000).
- Die Kirchen und der Rundfunk in Deutschland haben eigene Datenschutzbeauftragte (DSB).

Beispiel: LfD-SH bzw. ULD



Primäre Adressaten:			
	Öffentliche Verwaltungen	Wirtschaft, Wissenschaft, Verwaltung	43 Mitarbeiterinnen und Mitarbeiter, davon 7 im Projektbereich und 6 im Bereich Siegel/Audit
	Unternehmen		
	Bürger, Kunden, Klienten, Patienten		

Datenschutz: Geschichte und Medien

- *ab 1890* (Warren/Brandeis, USA): „**The right to be let alone**".
- *1960*: Missstände in Kreditwirtschaft, Einführung eines Melderegisters in den USA, in Deutschland Argwohn über Machtasymmetrie durch IT-Einsatz bzgl. Legislative / Exekutive.
- *ab 1970:* Erstes **Hessisches Datenschutz-Gesetz**, Einrichtung der Landes-DSBeauftragten.
- *1983*: **Volkszählungsurteil** des BVerfG: „Recht auf informationelle Selbstbestimmung".
- *ab etwa 1990*: Technisierung des Datenschutzes: „Privacy-Enhancing-Technologies" (PET): **Datenschutz mit Technik durchsetzen!** Ausbildung von Instrumenten des Systemdatenschutzes / Selbstdatenschutzes (z.B. Identitymanagement Typ3)
- *ab 2000*: Ökonomisierung des Datenschutzes, nachgewiesen guten **Datenschutz: gütesiegeln und auditieren.**
- *ab 2005*: „Datenschutz in die **Prozesse**!" CC, ITIL, CoBIT, BSI-GS, IFG-Bund, EuroPrise-Gütesiegel.
- *2008.02*: BVerfG: „Gewährleistungsgrundrecht auf **Integrität und Vertraulichkeit** informationstechnischer Systeme".
- *ab 2010*: Erweiterung und Spezifikation der Schutzziele der Datensicherheit durch die **Neuen Datenschutz-Schutzziele**: Nicht-Verkettbarkeit, Intervenierbarkeit, Transparenz.

1. Phase eines primär reaktiv und **normativ** ausgerichteten Datenschutzes
Kernfigur: Verbot mit Erlaubnisvorbehalt.

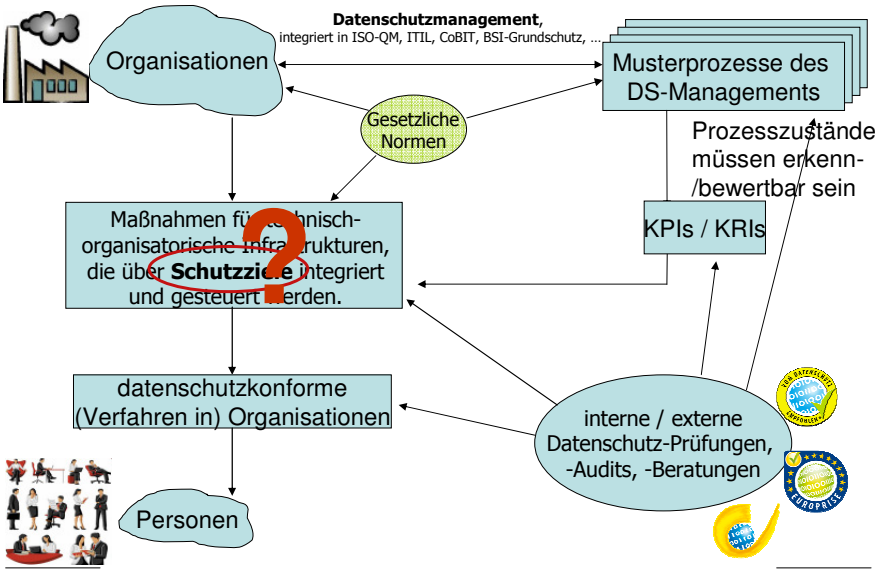
2. Phase eines zusätzlich proaktiv und **operativ** agierenden Datenschutzes

- **Privacy 1.0**: Datenminimierung, z.B. durch Anonymität
- **Privacy 2.0**: Nutzersteuerung durchIdentitätenmanagement sowie Datenschutzmanagement und Audits
- **Privacy 3.0**: Kontextuelle Integrität (Borcea-Pfitzmann et al. 2011)

2. Zwischenfazit

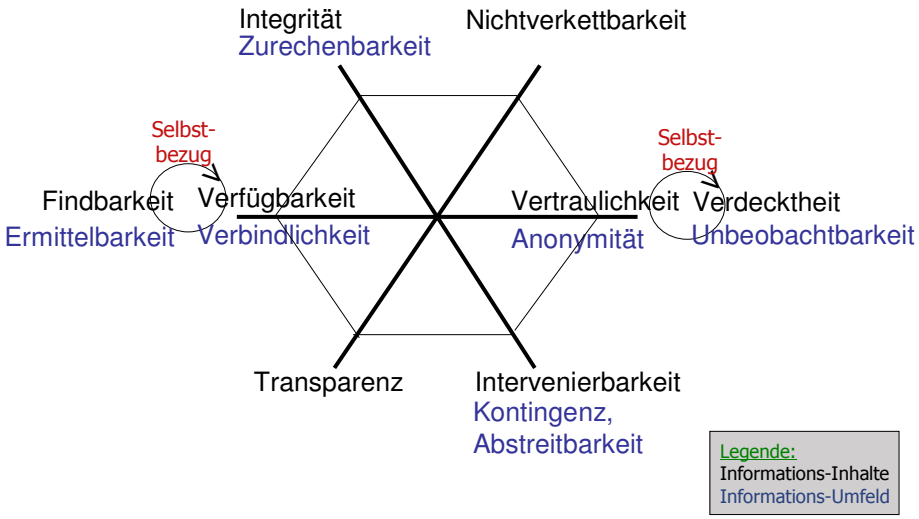
- Organisationen dürfen im Grundsatz keine personenbezogenen Daten verarbeiten.
- Die meisten Datenschutzregeln klären, unter welchen Umständen Organisationen ausnahmsweise personenbezogene Daten verarbeitet dürfen.
- Datenschutz hat sich von einer reinen juristischen Disziplin zu einer auch Technik einsetzenden Disziplin verändert: Datenschutz nicht gegen sondern durch die Nutzung von Technik (Privacy Enhancing Technologies) bzw. Identitätenmanagement.

Datenschutz: The big picture



Systematik der Datenschutzziele

(Entwickelt aus: Rost/ Pfitzmann, 2009: Schutzziele revisited; in: DuD 2009/06: 353ff)



Maßnahmen zur Umsetzung von Datenschutz

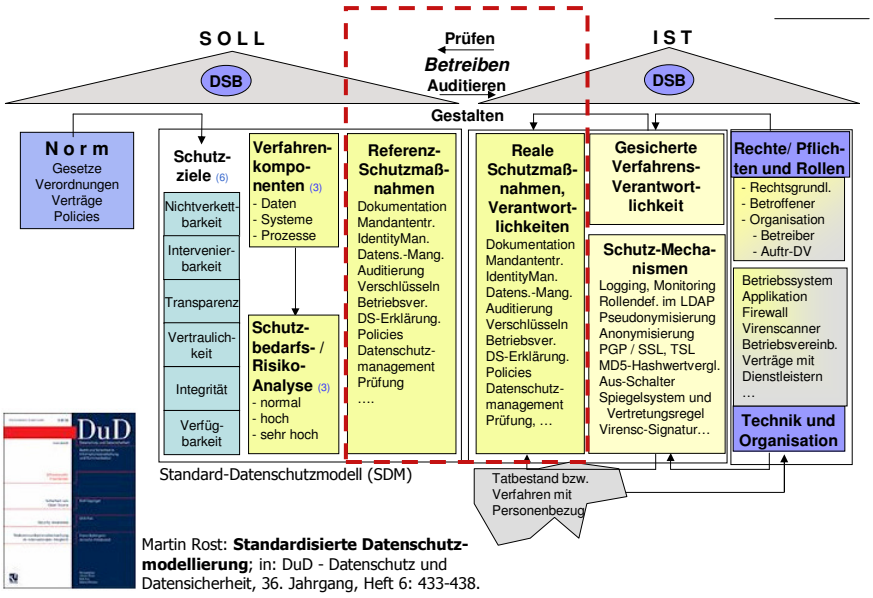
- **Sicherstellung von *Verfügbarkeit***
  Daten/Prozesse: Redundanz, Schutz, Reparaturstrategien
- **Sicherstellung von *Integrität***
  Daten: Hash-Wert-Vergleiche
  Prozesse: Festlegen von Min./Max.-Referenzen, Steuerung der Regulation
- **Sicherstellung von *Vertraulichkeit***
  Daten: Verschlüsselung
  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: Identitätenmanagement, 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,

Funktion der Schutzziele des Datenschutzes

- Die Schutzziele transformieren *wechselseitig normative und technisch-organisatorische Anforderungen* an technisch-organisatorische Systeme.
- Vertrauen zu gewähren und zu beanspruchen ist dann rational, wenn Organisationen gegenüber
  - sich selber,
  - den betroffenen Personen und
  - externen Aufsichtsinstanzen

  nachweisen (können), dass sie ihre Prozesse der Datenverarbeitung und ihre Systeme gemäß den von den Schutzzielen formulierten Anforderungen beherrschen und dabei generell an Fairness bzw. Rechtskonformität gegenüber Personen orientiert sind.
- Schutzziele operationalisieren iie Vertrauenswürdigkeit der Kommunikation zwischen Organisationen und deren Personen (Bürger, Kunden, Mitglieder, Personen).
- → Schutzziele transferieren ein Vertrauensproblem zwischen Organisationen und Personen in ein Entscheidungsproblem. ←

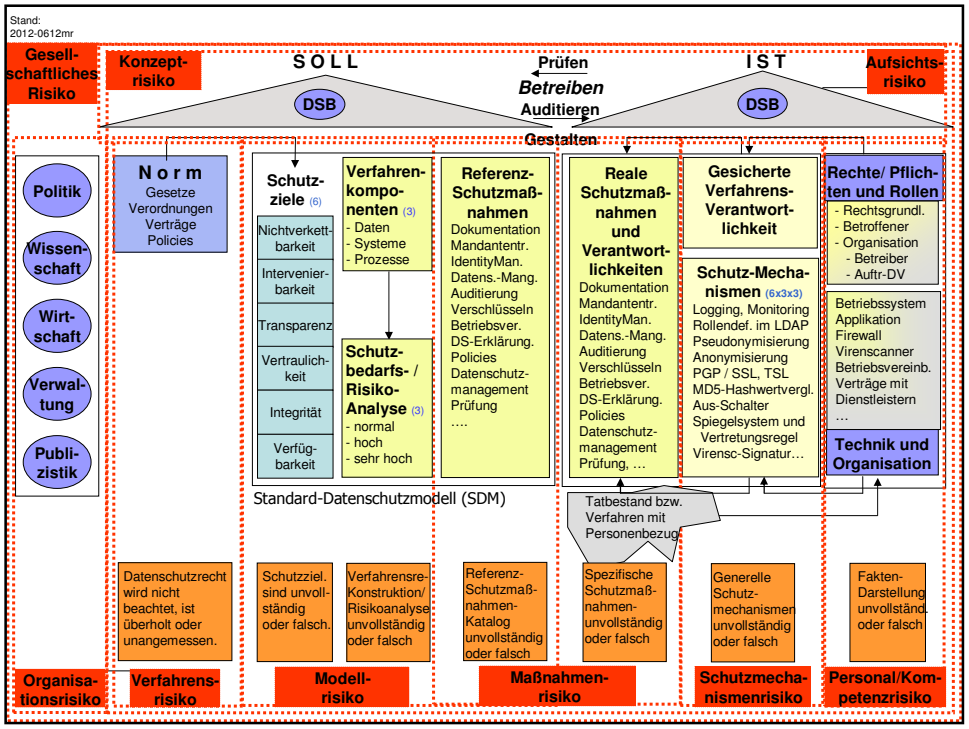
Datenschutz: umsetzen und prüfen



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

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



3. Zwischenfazit

- Das Konzept der Schutzziele („SZ“) sowie das Standard-Datenschutzmodell („SDM“) erlauben einen integren, transparenten und zweckgemäßen wechselseitigen Transfer zwischen rechtlichen Normen und technischen Funktionalitäten in Bezug auf die Gestaltung der Aktivitäten von Organisationen,
- SZ und SDM operationalisieren den Anspruch auf Beherrschbarkeit von Verfahren als Voraussetzung für Vertrauenswürdigkeit und Fairness in der Beziehung zwischen Organisationen und deren Klientel.

Datenschutzanalyse von facebook gem. SZ

- Keine Zusicherung der Verfügbarkeit des Dienstes für Nutzer oder Kunde.
  Der Dienst kann jederzeit beendet werden.
- Keine Zusicherung der Integrität sämtlicher Daten, insbesondere der Profildaten.
  Es können Personeneigenschaften beliebig verändert werden.
- Keine Zusicherung der Vertraulichkeit von Daten und Kommunikationen insbesondere gegenüber Facebook und deren Kunden.
  Personbezogene Daten sind verfügbar für den der zahlt (Marketing) oder sie beschlagnahmt (Staat)
- Keine Zusicherung von Transparenz darüber, was Facebook mit Daten macht.
  Keine Prüffähigkeit der Datenverarbeitung von Facebook.
- Keine Zusicherung bzgl. der Nicht-Verkettbarkeit, zu welchem Zweck Facebook die Daten erhebt.
  Facebook speichert und verkettet sämtliche personenbezogene Daten ohne festgelegten Zweck.
- Keine Zusicherung von Intervenierbarkeit des Nutzers in seine eigene Datenverarbeitung auf Facebook.
  Nutzer kann seine Daten weder löschen

Datenschutzanalyse von facebook gem. SDM

- Sehr hoher Schutzbedarf (existentielle Bedrohung siehe „Arabischer Frühling“) der Daten bzw. des Dienstes
- Modellierung der Daten, IT-Strukturen und Prozesse mangels Transparenz (kein Zugriff auf Dokumente und Protokolle durch Nutzer oder Aufsichtsbehörden) unklar.
- Kein methodischer Soll-Ist-Abgleich möglich, damit ist keine Prüffähigkeit des Dienstes gegeben.
- Einwilligung ist nicht rechtskonform, weil nicht hinreichend informiert und bestimmt und die Grundrechte nicht achtend (z.B. Unverletzlichkeit des Briefgeheimnises (Art. 10 GG)).
- Fazit: Facebook agiert nicht rechtskonrom, da Verstoß gegen Datenschutzrecht und nicht bereit oer unfähig nachzuweisen, dass es seine Prozesse beherrscht.

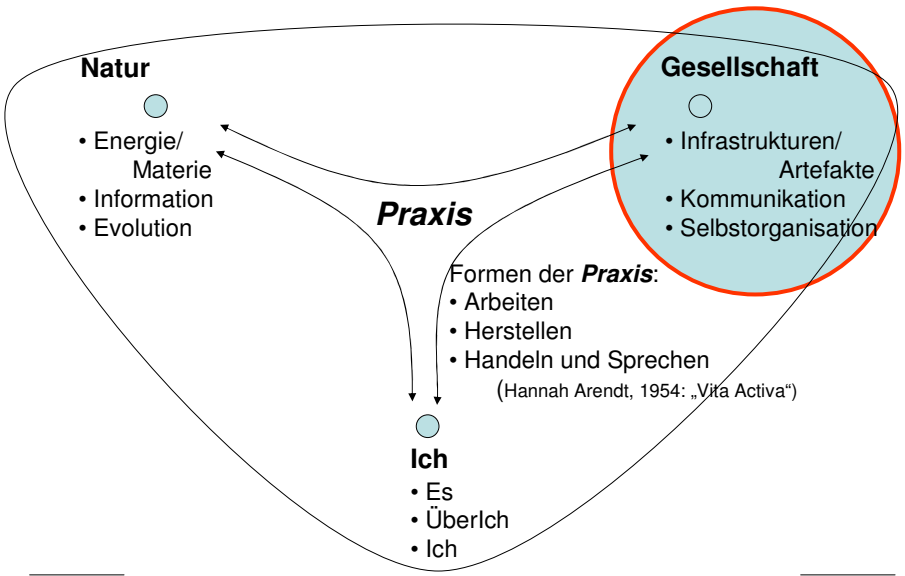
Was meint Soziologie?

Soziologie: Was ist Gesellschaft?

- „Gesamtheit der Produktionsverhältnisse“
  Marx 1857/58: Grundrisse
- „Gemeinschaft und Gesellschaft“
  Tönnies (1887): Gemeinschaft und Gesellschaft
- „Realität sui generis“
  Durkheim 1897: Regeln der soziologischen Methode
- „Formen der Wechselwirkung handelnder Personen“
  Simmel 1918: Soziologie
- „Emergente Figurationen“
  Elias 1936: Prozess der Zivilisation
- „Handlungssystem“
  Parsons 1937: Structure of social action
- „Konstruktion der Wirklichkeit“
  Berger/ Luckmann 1966: Gesellschaftliche Konstruktion der Wirklichkeit
- „Soziale Felder“
  Bourdieu 1979: Die feinen Unterschiede
- „System und Lebenswelten“
  Habermas 1982: Theorie des kommunikativen Handelns
- „Selbstreproduzierende Kommunikationssysteme“
  Luhmann 1998: Soziale Systeme

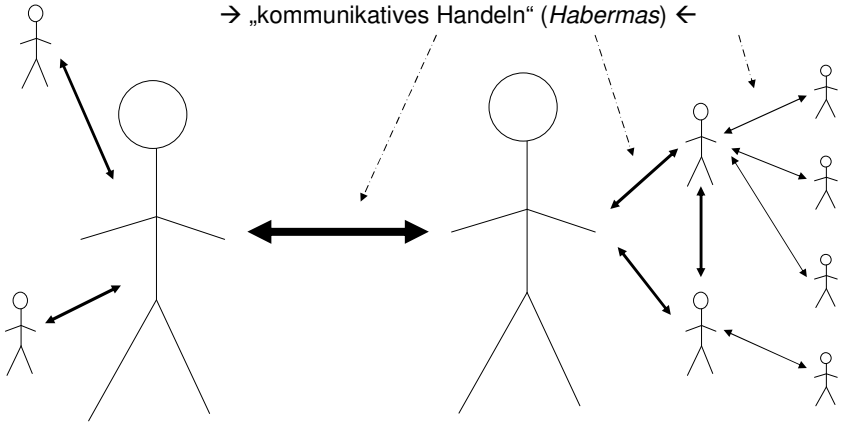
3-Welten-Theorie

(in Anlehnung an Popper, konventionelle Ontologie)



„Klassischer“ Objektbereich der Soziologie

„Formen der Wechselwirkung“ (*Simmel*) als „emergente Figuration“ (*Elias*) oder als „Realität sui generis“ (*Durkheim*).
→ „kommunikatives Handeln“ (*Habermas*) ←



Die „Pfeile“ bilden den Kernbereich „des Gesellschaftlichen“!

4. Zwischenfazit

Die Soziologie nimmt nicht „den Menschen“ in den Blick, auch nicht irgendwie „die Menschen“, sondern diejenigen Formen, die das Handeln und Sprechen von Menschen konstituieren und beschränken und sich eigensinnig verstetigt haben.

Formen sozialer „Beziehungen“

(„Evolution sozialer Systeme“ nach Luhmann 1998)

- **Gemeinschaften, mit Segmenten**
  - Horden, Clans, Verwandtschaft und Familien
  - geringe Rollendifferenzierungen/ Rollenkonflikte, Primat Sachorientierung
- **Organisationen mit Hierarchien (Stratifikation)**
  - Burgen, Schiffe, Manufakturen, Militärs, Klöster
  - komplexe Rollendifferenzierungen/Rollenkonflikte, Primat Sozialorientierung, Ringen mit formaler Logik
- **Moderne Gesellschaften mit funktionaler Differenzierung**
  - Moderne Gesellschaften entstehen im Vorlauf der Industrialisierung. Entwicklungen: Buchdruck, technische Zeichnungen, Blaupausen, Buchgeld, Kapitalverzinsung, Macciavelli, Hobbes Leviathan, Trennung Religion-Politik, philosophisch-aufklärerische Selbstbewegungslogiken philosophisch durchdekliniert für Natur (Schelling), Ich (Fichte, Kant), Gesellschaft (Hegel, Marx)
  - Keine zentral-logische Vereinbarkeit verschiedener Rollen mehr, Primat der Orientierung an Zeit und punktueller Ereignishaftigkeit

Soziale Systeme moderner Gesellschaften

(nach Luhmann 1998)

- **Interaktionssysteme**
  - Anwesenheit unter Personen
  - Kommunikationsmedium: Rede
  - Reproduktion von Aufmerksamkeit
- **Organisationssysteme**
  - Mitgliedschaft, Kommunikation über Entscheidungen und Entscheidungsprogramme
  - Kommunikationsmedium: Schrift
  - Verwaltungen, Firmen, Vereine, Kirchen...
    - Reproduktion von Adressierbarkeiten, Rollen und Funktionen
- **Gesellschaftliche Funktionssysteme**
  - Kommunikative Erreichbarkeit
  - Kommunikationsmedium: Symbolisch generalisierte, binäre Schematismen:
    - Wirtschaft (Zahlung/Nichtzahlung, Schema: Preise),
    - Politik (Macht/Nichtmacht, Schema: politische Programmatiken),
    - Recht (Recht/Nichtrecht, Schema: Gesetze),
    - Wissenschaft (Wahr/Nichtwahr, Schema: Theorien und Methoden)

Gesellschaftliche Funktionssysteme und deren Kontingenz-Quellen

- Gesellschaftliche Funktionssysteme haben spezifischen Kontakt nur zu sich selbst. Es gibt keinen Import von Informationen, „operativer Blindflug über den Wolken“.
- Sozialsubsysteme können andere (auch Sozial-)Systeme nur als Störungen in ihrer Umwelt wahrnehmen.
- Die gesellschaftlichen Sozialsysteme müssen die externen Umweltstörungen in interne Informationen transformieren und halten sich zudem an ihre systemeigenen Quellen einer systemimmanenten Verunsicherung genauer: Kontingenz (offene Nicht-Notwendigkeit). Die Verunsicherungsquellen sind:
  - Politik: **Gewaltenteilung, öffentliche Meinung, Bewegungsfreiheit**
    Rolle *Staats-Bürger („citoyen“)*
  - Justiz: **Gewaltenteilung, Grundrechte** als Abwehrrechte gegenüber dem Staat
    Rolle: *Polit-Bürger („bourgeois“)*
  - Wirtschaft: **Markt, Eigentum**
    Rolle: *Kunde*
  - Wissenschaft: **Diskurs**, **Wissen**
    Wissen führt nicht zur Gewissheit, sondern zur erweiterten Ungewißheit
    Rolle: *Mensch* (Medizin, Anthropologie, Biologie), *Subjekt* (Philosophie), *Individuum* (Psychologie), *Person / Unjekt* (Soziologie)
  - Kunst: **Opposition zum Nützlichen**, Perspektivenvielfalt, Konstruktivität, Transzendenz
    Rolle: *Produzent/Rezipienten, Prosumer (Internet)*

5. Zwischenfazit

- Es gibt drei Typen sozialer Systeme
  - Interaktionssysteme
  - Organisationssysteme
  - Funktionssysteme
- Die Funktionssysteme haben ihre systemeigenen Quellen der „Störung“ und „Verunsicherung“, die dann bestimmte Anforderungen an Personen stellen:
  - Politik/ Recht – Politische Teilhabe, Gewaltenteilung – Behörden -> Bürger
  - Wirtschaft – Markt – Unternehmen –> Kunden
  - Wissenschaft – Diskurse - Institute -> Mensch, Subjekt, Individuum, Person
  - Kunst – Werke – Museen –> Künstler

Geltungsansprüche

(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. **Solange die Verständigung gelingt, bleiben die wechselseitigen Ansprüche unthematisiert, scheitert sie, müssen die Unterstellungen daraufhin überprüft werden, welche von ihnen unerfüllt blieb. Je nach Geltungsanspruch existieren unterschiedliche Reparaturstrategien.**

Habermas unterscheidet vier Arten von Geltungsansprüchen sinnhafter Rede, 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.“

Datenschutzsoziologische Analyse von facebook II

- Facebook agiert nicht datenschutzgerecht und ist demnach nicht vertrauenswürdig. Es ist nicht rational und im Sinne Habermas nicht vernünftig, die Dienste von Facebook zu beanspruchen.
- Facebook unterläuft die Mechanismen des Marktes (sämtliche Aktivitäten von Angebot und Nachfrage werden zentral gespeichert und analysiert, kein anonymes Bezahlen), des Rechtsstaates (keine Gewaltenteilung, keine anonyme Abstimmbarkeit) und auch den wissenschaftlich-freien Diskurs (keine anonyme Teilnahme a la „anonymous peer reviews“ mit der Chance auf Freisetzung des „seltsamen Zwangs des besseren Arguments“ (Habermas)).
- Facebook agiert als eine dem Markt und dem Recht weitgehend entzogene zentrale Vermittlungsinstanz und ist dadurch ein organisierter Angriff auf die funktionale Differenzierung moderner Gesellschaften.
- **Reichen diese Befunde für Faschismusverdacht gegenüber facebook** (und nicht minder gegenüber google, apple)?

Zur gesellschaftliche Funktion des Datenschutzes

Datenschutz ist die organisierte Beobachtung der Differenz Organisation vs funktional. Differenzierung

- Organisationen brechen latent die Kontingenzquellen und Freiheitsversprechen der Funktionssysteme:
  - Monopolisierung anstatt Markt,
  - Dominanz der Exekutive anstatt Gewaltenteilung und Mitbestimmung auch der Schwachen,
  - Diskursimmunisierung anstatt Diskurs,
  - Bändigung der Formenvielfalt anstatt Variationenfülle
- Am Brechen der Souveränitätsversprechen gegenüber Bürgern, Kunde, Subjekten, Individuen…, detektiert Datenschutz nicht funktionierende Differenzierung durch überdominant agierende Organisationen.
- Datenschutz interveniert in Organisationen, damit diese die Souveränität von Personen achten und somit funktional-differenziert agieren.
- Die Interventionen des DS geschehen entlang der Schutzziele.

Schutzziele als Geltungsanforderungen an vernünftiges Operieren organisierter Systeme

- Geltungsanforderungen an kommunikatives Handeln (Verständlichkeit, Wahrheit, normative Richtigkeit, Wahrhaftigkeit) zielen auf Konsensfähigkeit ab. Man kann deren grundlegende Geltung für vernünftig auf der **Sinnebene** funktionierender Kommunikation nicht aussichtsreich bestreiten.
- Die Schutzziele des Datenschutzes (Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit, Intervenierbarkeit) stellen auf ein vernünftiges Funktionieren technisch-organisatorischer Systeme ab. Man kann deren Geltung für vernünftig auf der **operativen Ebene** funktionierende Kommunikation diskursiv nicht aussichtsreich bestreiten.

Folgerungen für die Gestaltung von IKT in einer modernen Gesellschaft

1. Die Umsetzung der Schutzziele des Datenschutzes ist eine Voraussetzung dafür, dass Kommunikation verallgemeinerungsfähig vernünftig gelingen kann. Das heisst: **Kommuniktions- und Informationstechnik muss neutral funktionieren und darf niemanden strukturell bevorteilen, auch wenn sie von Organisationen erbracht und genutzt wird**.

2. Wenn die Definition von Menschenwürde nicht mehr christlich (wie noch im maßgeblichen GG-Kommentar Dürig/Maunz bis 2003), sondern als „kommunikativ eingebettet“ begriffen wird (GG-Kommentar Dürig/Maunz nach 2003), dann folgt daraus, **dass eine unfaire ausgelegte und technisch unbeherrscht und unsicher betriebene I&K-Technik strukturelle Risiken für die Würde des Menschen erzeugt.**

Kontakt?

Vielen Dank für
Ihre Aufmerksamkeit

Literaturhinweis

Martin Rost:
Soziologie des
Datenschutzes,
in: DuD 2013/02: 84-89.

Martin Rost

Mail: martin-rost@web.de
Webseite: http://www.maroki.de
Blog: https://marokiblog.wordpress.com
Twitter: http://twitter.com/#Martin_Rost