Informatik und Gesellschaft
[Computers and Society]

Stefan Köpsell
TU Dresden, Fakultät Informatik, Lehrstuhl Datenschutz & Datensicherheit
Dresden, Nöthnitzer Str. 46, Raum 3062
Tel.: +49 351 463-38272, E-Mail: stefan.koepsell@tu-dresden.de, https://dud.inf.tu-dresden.de/iug
(Folien zur Modellbildung von Andreas Pfitzmann)

Allgemeine (organisatorische) Hinweise

- Web-Seite: dud.inf.tu-dresden.de/iug
- Materialien auf der Web-Seite stammen zu Teilen von Prof. Pfitzmann
- „Skript“ ist eher eine Sammlung von Notizen – aber lesenswert…
- Mailingliste:
  - OPAL!
- Einschreiben in OPAL
- Abschluß:
  - unbenoteter Schein für **aktive** Teilnahme + kurzes Gespräch
  - für Note zusätzlich: Prüfung
    - 3 Themen wählen

Ergebnis der Lehrveranstaltung (aus Sicht der Studierenden)

- nützlicher Erkenntnisgewinn
- nette Diskussionen

- Abrechenbar mit Note im Rahmen der Fachprüfung

- Abrechenbar mit Schein
  - erfordert aktive Teilnahme des Studierenden an der LV

Ablauf der Lehrveranstaltung

- im Wesentlichen bestimmt durch die Studierenden
- Rahmenideen:
  - Vorträge von *externen Experten* zu bestimmten Thematiken mit Bezug zu „Informatik und Gesellschaft“
    - Datenschutzrecht, Gesellschaft und soziale Systeme, Gremien und Organisationen…
  - Beiträge von Studierenden
    - Rahmen: Podiumsdiskussion zu gegebener Thematik
    - 3-5 Teilnehmer (1 Moderator)
    - mögliche Aufteilung:
      - 1 x Impulsreferat (max. 30 min)
      - 2-4 x kurze Statements [pro & contra] (ca. 5 min)
    - Diskussion der Teilnehmer mit Auditorium unter Leitung des Moderators

Ablauf

Datum	Veranstaltung
10. Apr	Einführung / Themengenerierung
17. Apr	Themenvergabe / Modellbildung / Rebound-Effekt / Vertrauen / Technikfolgenabschätzung
24. Apr	Autonomes Fahren
1. Mai	**Tag der Arbeit**
8. Mai	Deep Fakes
15. Mai	Dark Patterns
22. Mai	**Pfingsten**
29. Mai	Informatik und Bildung
5. Jun	**Dies Academicus**
12. Jun	Medienkonsum
19. Jun	Datenschutz
26. Jun	AI
3. Jul	Diversity & AI
10. Jul	Umwelt
17. Jul	Fallbeispiele oder anderes Thema?

Thematik der Lehrveranstaltung

- Informatik **und** Gesellschaft
  - im Wesentlichen geht es um das „und“…
  - … wobei ggf. auch diskutiert werden kann, ob man „*und*“ besser ersetzen sollte durch: „*oder*“, „*trotz*“, „*wegen*“ etc.
  - Wechselwirkung von Informatik und Gesellschaft

Zum Begriff „Informatik“ (computer science)

- „*Wissenschaft, die sich mit den theoretischen Grundlagen, den Mitteln und Methoden sowie mit der Anwendung der Elektronischen Datenverarbeitung (EDV) beschäftigt, d. h. mit allen Aspekten der Informationsverarbeitung unter Einsatz von Computern* ***einschließlich ihres Einflusses auf die Gesellschaft***“ [Taschenbuch Informatik, 2006]

Zum Begriff „Informatik“ (computer science)

- „***Informatik*** *ist die ‚Wissenschaft von der systematischen Verarbeitung von Informationen, besonders der automatischen Verarbeitung mit Hilfe von Digitalrechnern.‘* “
  [Wikipedia, 4. April 2013, Zitat übernommen aus Duden Informatik]

- „***Informatik und Gesellschaft*** *(IuG) ist ein Teilbereich der Wissenschaft Informatik und erforscht die Rolle der Informatik auf dem Weg zur Informationsgesellschaft.*“
  [Wikipedia, 4. April 2013]

Zum Begriff „Informatik“ (computer science)

- *„Computer science is the study of the theory, experimentation, and engineering that form the basis for the design and use of computers. It is the scientific and practical approach to computation and its applications…“*

  [Wikipedia, 8. April 2018]

  – „Computers and Society“ nicht erwähnt

- Was ist Informatik? Positionspaper der Gesellschaft für Informatik [https://gi.de/fileadmin/GI/Hauptseite/Themen/was-ist-informatik-lang.pdf]

  – Grundlagenwissenschaft, Ingenieurdisziplin, Experimentalwissenschaft, Innovationsmotor und Einflußfaktor für Wissenschaft, Wirtschaft, Bildung, Kultur und Gesellschaft

Zum Begriff „Gesellschaft“

- „*Die Chance oder der Alptraum, wie Menschen, in ihrer Basisfunktionalität also höhere Säugetiere, human hoffentlich mehr mit als gegeneinander leben können.*“ [Andreas Pfitzmann, IuG Skript]
- „*zweckgebundene, aus Nützlichkeitserwägungen entstandene, meist in sich gegliederte Gruppe von Menschen, die zusammen leben und arbeiten.*“ [Großes dt. Wörterbuch, 1973]
- Begriffe & Konzepte:
  - Gesellschaftssysteme, Gesellschaftsstruktur, Sozialstruktur, Gesellschaftsordnung, pluralistische Gesellschaft, Interessenausgleich, Weltanschauung, Religion

Zum Begriff „Gesellschaft“

- „*die im staatlichen, wirtschaftlichen und geistigen Leben zusammenwirkende Gesamtheit der Individuen als Träger der sozialen Beziehungen*“ [Meyers Großes Handlexikon, 1991]
- „*Gesamtheit gesellschaftlicher Verhältnisse, also der Beziehungen, die durch das wechselseitige Handeln der Menschen und ihrer Organisationen entstehen. Sie beruht auf einem bestimmten geschichtlichen Entwicklungsstand der Produktivkräfte und dem ihnen entsprechenden System der Produktionsverhältnisse*“ [Jugendlexikon, DDR, 1987]
- „*Produkt des wechselseitigen Handelns der Menschen.*“ [Karl Marx, 1846]

„Informationsgesellschaft“

- „Der Begriff *Informationsgesellschaft* bezeichnet eine auf Informations- und Kommunikationstechnologien (IKT) basierende Gesellschaft. Der Prozess der Durchdringung aller Lebensbereiche mit IKT, durch den sich eine postindustrielle oder postmoderne Informations-gesellschaft bildet, wird als *Informatisierung* bezeichnet (Nora/Minc 1979). Der Begriff Informationsgesellschaft ist nicht starr definiert und wird oft mit dem Begriff der *Wissensgesellschaft* zusammen verwendet “

  [Wikipedia, 23. März 2011]

- …wenn auch nicht klar ist, was „Informationsgesellschaft“ ist, so hat es doch sicher etwas mit „Informatik und „Gesellschaft“ zu tun…

Thematik der Lehrveranstaltung

- Informatik **und** Gesellschaft
  - im Wesentlichen geht es um das „und“…
  - … wobei ggf. auch diskutiert werden kann, ob man „*und*“ besser ersetzen sollte durch: „*oder*“, „*trotz*“, „*wegen*“, „*für*“, etc.
  - Wechselwirkung von Informatik und Gesellschaft

  - umfassende „Definition“ existiert nicht (bzw. ist mir nicht bekannt)
  - beschreibender Erklärungsversuch: *siehe Taschenbuch Informatik, 2006, Kapitel 1.5, S. 33ff*
  - …ein weites Feld, daß hier sicher nicht umfassend behandelt wird
    - vielmehr soll an ausgewählten Beispielen für die Thematik sensibilisiert werden

Themenvorschläge

- Informatik & Infrastruktur
  - **Cloud-Computing: Vorteile? Nachteile? Datenschutz?**
  - **Netzneutralität?**
  - **Netzversorgung: Grundrecht? Menschenrecht? rein marktwirtschaftlich geregelt?**
  - Einfluß der Informatik auf Infrastrukturen: Telefon (VoIP), Strom (Smart Grid)
  - Verbesserung / Verschlechterung bezüglich Verletzbarkeit der Gesellschaft?
  - Robustheit? Verfügbarkeit?

Themenvorschläge

- **Informatik & Menschen mit Behinderung**
  - Behinderung – relevantes Thema für Informatik?
  - Behinderung & Benutzbarkeit; Richtlinien und gesetzliche Regelungen
  - Berücksichtigung in der Ausbildung?
  - soziale Ausgrenzung

Themenvorschläge

- Informatik & alte Menschen
  - ambient assisted Living
  - Dauerüberwachung vs. Datenschutz
  - spezielle Geräte? Software? Dienste?
  - **Ausgrenzung älterer Menschen?**
  - **„digital natives“ vs. „digital immigrants“**
  - **„digital divide“**

Themenvorschläge

- Informatik & Ethik
  - ethische Richtlinien / Codes of Conduct: welche gibt es? sind sie sinnvoll? sollten sie überhaupt existieren?
  - **gesetzliche Regelungen?**
  - Erkenntnisgewinn um jeden Preis?
  - Technological determinism / Technological neutralism
  - **Implantate = Cyborgs als Supermenschen von morgen?**
  - **Verantwortung von Informatikern / Softwareentwicklern**
    - **(Software-)Entwicklung für Waffen**
    - **bewußt / unbewußte Unterstützung (Stichwort: Dual-Use)**
  - **„Hackerparagraph“**
  - penetration tests
  - social engineering

Themenvorschläge

- **Robotergesetze**
  - was ist das? was soll das?
  - ursprüngliche Version der asimovschen Gesetze
  - Erweiterungen & Ergänzungen
  - Bezug zur Informatik, Praxisrelevanz
  - ELROB, DARPA „Grand Challenge“
  - „Smart Dust“
  - Maschinenethik: „Debatte rein akademischer Natur.“ [Colin Angle in Technology Review Interview (http://www.heise.de/tr/artikel/Die-Ethik-Debatte-ist-unnoetig-963020.html)]?
  - Lehrveranstaltung „Robots and Socitety“ [Ronald Arkin (http://www.cc.gatech.edu/classes/AY2010/cs4002_spring/)]

Themenvorschläge

- **Künstliche Intelligenz**
  - was ist das? was soll das?
  - **Künstliche Intelligenz: wünschenswerter Traum oder Horrorvision?**
  - **Grenzen des Einsatzes von KI aus ethischen Gründen**
  - **psychologischer Einfluß**
  - **Verlassen auf IT**
    - **Beispiel: autonomes Fahren**
  - **Entmündigung von Menschen?**
  - **Entlastung von Menschen?**
  - **!Verantwortung!**

Themenvorschläge

- **Computerspiele**
  - **„Killerspiel“ Debatte: Wahrnehmung von Computerspielen in der Gesellschaft**
  - Regulierung notwendig?
  - **Suchtpotential und –gefahr?**
  - Bildungseffekte?
  - sozial Kompetenz?
  - online (Glücks)spiele
  - Demographischer Wandel ←→ Zielegruppe Computerspiele
  - Gameifikation (Spiele als Motivation)
  - In-App Käufe / Free-toPlay → Einfluß Kinder
- Informatik & Medien(konsum)
  - sinnvolle Informationsgewinnung
  - Verdrängung klassischer Medien
  - Überlastung durch Informationsflut
  - Verhaltensveränderung (Konzentration / Aufnahmefähigkeit / Ablenkung)

Themenvorschläge

- Soziale Netze im Internet / Web 2.0.
  - was ist das? was soll das? braucht mensch das?
  - Vorteil / Nachteile
  - geschichtliche Entwicklung & zukünftige Trends
  - staatliche Regulierung?
  - Nutzungskontrolle von Kindern durch Eltern?
  - Blogs
  - Wikipedia
  - **Datenschutz?**
  - **Einfluß der Informatik auf das Kommunikationsverhalten? positiv? negativ?**
  - **Ableitung neuer sozialer Normen?**
  - **Onlinesucht?**

Themenvorschläge

- Informatik & Politik / politische Einflußnahme
  - **wieviel Ahnung haben Politiker von Technik? müssen sich daher Informatiker in Politik einmischen?**
  - Terrorismus & Anti-Terrorismus
  - „Facebook-Revolution“
  - **Zensur- & Anti-Zensurmaßnahmen**
  - „Cyberwar“
  - e-Government, e-Democracy
  - Adhocracy / Liquid Democracy
  - **Piraten Partei / GI / Bitkom / CCC / FoeBud / FifF**
  - Wikileaks, Anonymous
  - (Diebold-)Wahlmaschinen, Internet-Wahlen
  - Verläßlichkeit von Informationen
  - Einfluß auf Journalismus
  - Machtkonzentration bei privaten IT-Firmen

Themenvorschläge

- Informatik & Kunst, Kultur
  - Einfluß der Informatik auf die Kultur: positiv? negativ? unbedeutend?
  - **Verdrängung traditioneller Kulturgüter: Bücher, Zeitschriften etc, ?**
  - **Informatiker = neue Iconen der Pop-Kultur (Beispiel: Steve Jobs)?**
- **Urheberrecht** / geistiger Eigentum
  - (illegales) Filesharing
  - Kulturflatrate
  - Internetsperren
  - Anti-Counterfeiting Trade Agreement (ACTA)
  - überkommen Regelung für Internet- / Informationszeitalter
  - **Software Patente**

Themenvorschläge

- Informatik & Wirtschaft
  - Einfluß der Informatik auf die Wirtschaft: positiv? negativ? unbedeutend?
  - **Informatik = Jobkiller?**
  - **Informatik = Jobmotor?**
  - **Einfluß auf die Produktionsverhältnisse?**
  - neue Wirtschaftszweige und Wertschöpfungsketten?
  - Chance für Deutschland?
  - Outsourcing?
  - rasante Entwicklungsgeschwindigkeit = Jobende mit 40?
  - Wirtschaftsspionage
  - Arbeitsbedingungen bei Hardware- /softwareproduzenten
  - Einfluß auf Umweltschutz
  - Arbeitserleichterung?
  - Schnelligkeit der Datenverarbeitung
  - Big Data / Öl? / negative Einflüße?
  - Außendarstellung / shit storms

Themenvorschläge

- **Informatik & Datenschutz**
  - Informatik = Förderer des „gläsernen Menschen“?
  - Datenschutz: Datenschutzmodelle, Techniken, Gesetze
  - Nutzen von Datenschutz?
    - negativer Einfluß von Datenschutz
  - Datenschutz = Täterschutz?
  - Datenschutz = Innovationshemmnis?
  - Datenschutzprobleme: Mobiltelefone, soziale Netze, Web 2.0
  - Datenschutz: Fluch oder Segen?
  - staatliche Überwachung
  - Grenzen von Kryptographie
  - Verbergen der eigen Identität
  - Anonymität im Internet
    - Beeinflussung von Menschen

Themenvorschläge

- Informatik & Recht / Rechtssicherheit / Verbrechen
  - **„rechtsfreie Räume“? was ist das? gibt es das? positiv? negativ?**
  - Internet = „öffentlicher Raum“?
  - **Hacking**, Phishing
  - Viren, Würmer, Trojaner
  - digitale Forensik
  - Vorratsdatenspeicherung
  - Web-Sperren
  - Telekommunikationsüberwachung
  - Datenschutz
  - Biometrie
  - Bundestrojaner
  - De-Mail
  - neuer Personalausweis / Reisepaß
  - Social engineering
  - **„Hackerparagraph“**
  - INDECT-Projekt

Themenvorschläge

- Informatik & Fehler
  - Fehler in der Informatik / in Informationssystemen
  - Prinzipielle Fehlerhaftigkeit; Modellierung
  - Fehlertoleranz
  - Verletzlichkeit / Abhängigkeit der Gesellschaft
  - Hardware- / Softwarefehler
  - Fehlerarten
  - Verantwortung für Fehler
  - Risikomanagement
  - Business continuity, desaster recovery
  - Einfluß Energieversorgung < -- > Informatik

Themenvorschläge

- Informatik & Frauen
  - Informatik(er) = abschreckend für Frauen?
  - Informatik = Bastelspaß für große Jungs?
  - Frauenquote?
  - getrenntgeschlechtliche Ausbildung?
  - Änderungen in Schule, Kindergarten?

Themenvorschläge

- Informatik & Entwicklungsländer
  - spezifische Probleme / Situation
  - One Laptop per Child
  - Lizenzkosten
  - Hardwareanforderungen
  - **„digital divide“**

Themenvorschläge

- Informatik & Bildung
  - Informatikausbildung in der Schule? im Kindergarten?
  - Wahlfach? Pflichtfach? Umfang? Lehrinhalte?
  - Computer & Kinder: ab welchem Alter? Nutzungsumfang?
  - e-Learning
  - mehr / bessere Bildungsangebote?
  - Medienbildung / Medienkompetenz?
  - klassische Bildung vs. Selbstbildung (Wikipedia)
  - Verläßlichkeit von Informationen
  - Widerspruch: vorhandenes Wissen ←→ faktisches/abrufbares Wissen: Verdummung?

Themenvorschläge

- „always Online“
  - Einfluß auf Arbeitswelt ←→ Freizeit
  - medizinischer Einfluß (drahtlos Kommunikation, Psyche)
  - wie hat sich Kommunikation geändert?
  - neue Kommunikationsformen?

- Ubiquitäre / eingebettet /Cyper-physical-Systems / Internet of Things
  - Fluch oder Segen?
  - Risiken, Chancen?
  - Akzeptanz?
  - Grenzen

Themenvorschläge

- Bild / Wahrnehmung der Informatik in der Gesellschaft
  - Verständnis von / über Informatik
  - Rolle der Informatik
  - geistige Barrieren
  - Abwehrhaltung gegenüber neuer Technik
  - digital natives vs. digital emigrants
  - Diskussion aktueller IT-Themen in der Gesellschaft:
    - wie verständlich machen?
    - wie mit dem aktuellen Wissenstand möglich?

Themenvorschläge

- Informatik & Philosophie
  - Veränderung des Weltbildes durch Informatik?
- Informatik & Forschung
  - neue Erkenntnisse mit Hilfe der Informatik
    - Beispiel: Medizin

Themenvorschläge

- Informatik & Einfluß auf Kinder
  - Medienkonsum etc.
  - Medienkompetenz
  - In-App Käufe
- Drohnen
  - automatisierte Kriegsführung
  - Beweisbare Verläßlichkeit der System(?)

Themenvorschläge

- OpenSource
  - was ist das? wem nützt es? warum gibt es das? wer macht es?
  - Lizenzmodelle & Konsequenzen
  - Software als Allgemeingut?
  - Feind der Softwareindustrie?
  - GPL = OpenSource Diktatur?
  - Übertragung auf andere Bereiche: OpenContent, OpenCar, OpenMoko, Open…
  - **Software Patente**
  - **Open Data**

Themenliste

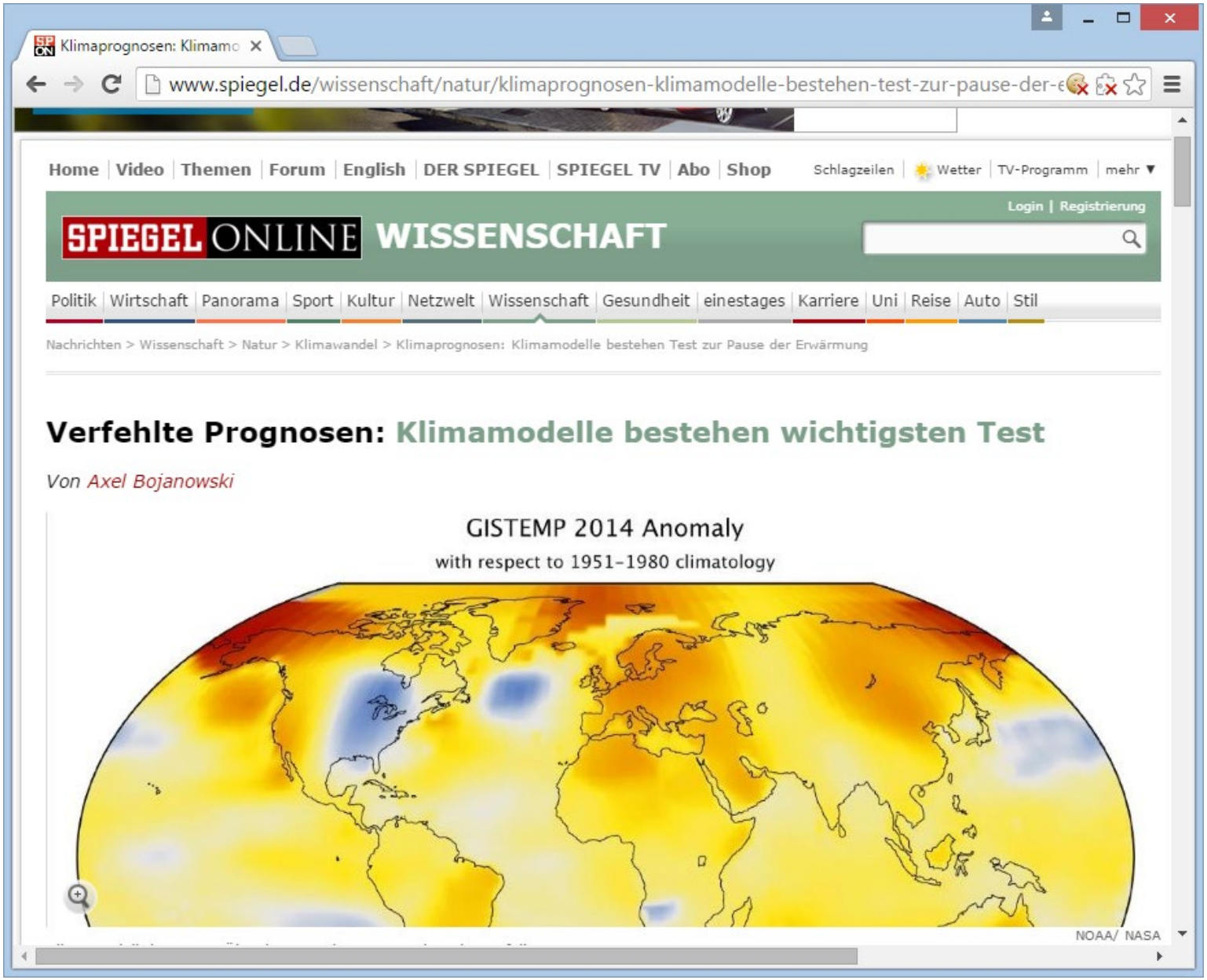
- Überwachung im Internet: Chatkontrolle/Vorratsdatenspeicherung
- Social Credit Systeme
- Datenschutz (unter anderem am Beispiel Google)
- Digital Service Act
- Informatik und Umwelt
- Informatik und Diversity: Diskriminierung durch KI
- Social Media im Hinblick auf psychische Gesundheit
- Fake News, Deep Fakes etc. (beispielsweise im Bereich Social Media)
- Informatik und Bildung: e-Learning, Digitalisierung in Schulen, Informatikbildung
- Dark Patterns, Meinungsbeeinflussung durch Personalisierung, Mikro targeting
- Medienkonsum, Einfluss auf Kinder
- Virtual Reality, XR, AR
- Einfluss von KI, Voice Assistance auf Bildung
- Autonomes Fahren, Schuldfrage
- Generative AI ←→ Persönlichkeitsrechte/Urheberrechte, AI und Kunst/Musik
- Anonymität im Internet
- Cyberware/ Cyberkriegsführung
- KI im Kriegseinsatz
- KI in der Justiz: KI als Richter, KI für Profiling in der Strafverfolgung
- Informatik in der Medizin: KI, Behandlung von Krankheiten
- Social Media – Einfluss auf soziales Zusammenleben

MODELLE ZUR WELTERKLÄRUNG

MODELLBILDUNG ALS HERRSCHAFTSINSTRUMENTE

TRAUE KEINER STATISTIK, DIE DU NICHT SELBST GEFÄLSCHT HAST

Modelle und Fehler



Modelle und Fehler

Klima: Gravierende Mänge

www.spiegel.de/wissenschaft/natur/klima-gravierende-maengel-bei-klimamodellen-entdeckt-a-1(

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop Schlagzeilen | Wetter | TV-Programm | mehr

Login | Registrierung

SPIEGEL ONLINE WISSENSCHAFT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Wissenschaft > Natur > Klimawandel > Klima: Gravierende Mängel bei Klimamodellen entdeckt

Fehler in Klimamodellen: "Dürreprognosen sind wenig vertrauenswürdig"

Von Axel Bojanowski

Modelle und Fehler

Antarktis-Eis könnte schne

www.spiegel.de/wissenschaft/natur/antarktis-eis-koennte-schneller-als-erwartet-schrumpfen-a-10

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop Schlagzeilen | Wetter | TV-Programm | mehr

Login | Registrierung

SPIEGEL ONLINE WISSENSCHAFT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

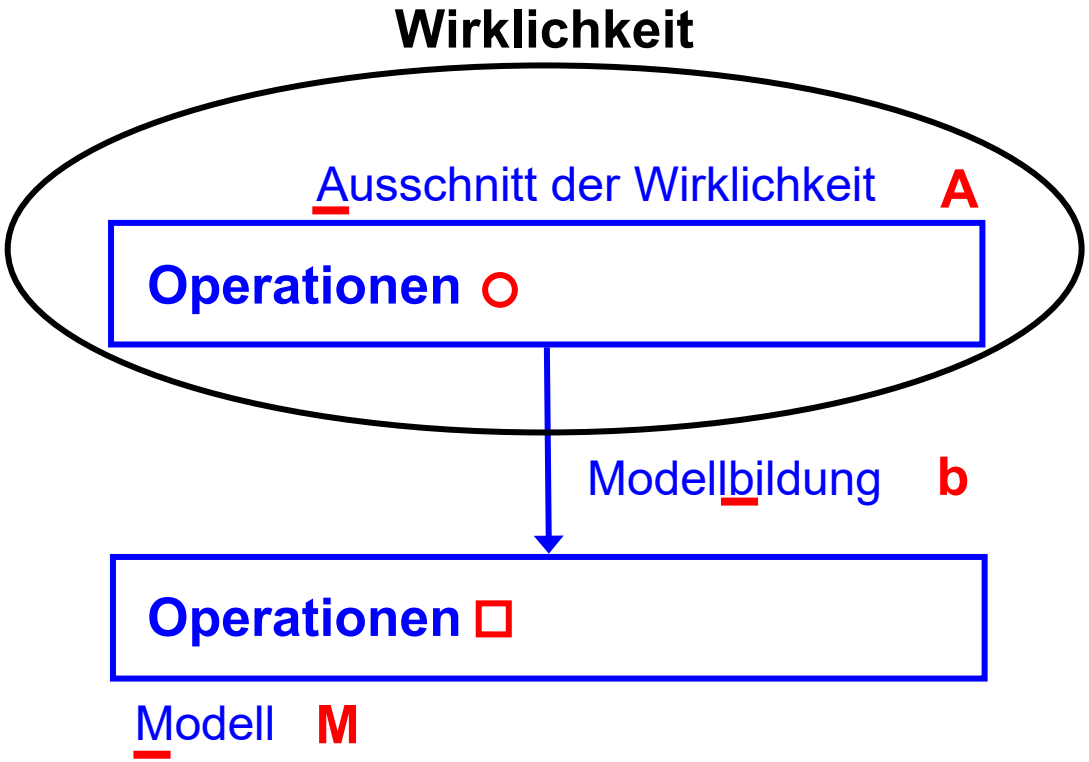
Nachrichten > Wissenschaft > Natur > Meeresforschung > Antarktis-Eis könnte schneller als erwartet schrumpfen

Klimaprognose: Antarktis-Eis könnte schneller als erwartet schmelzen

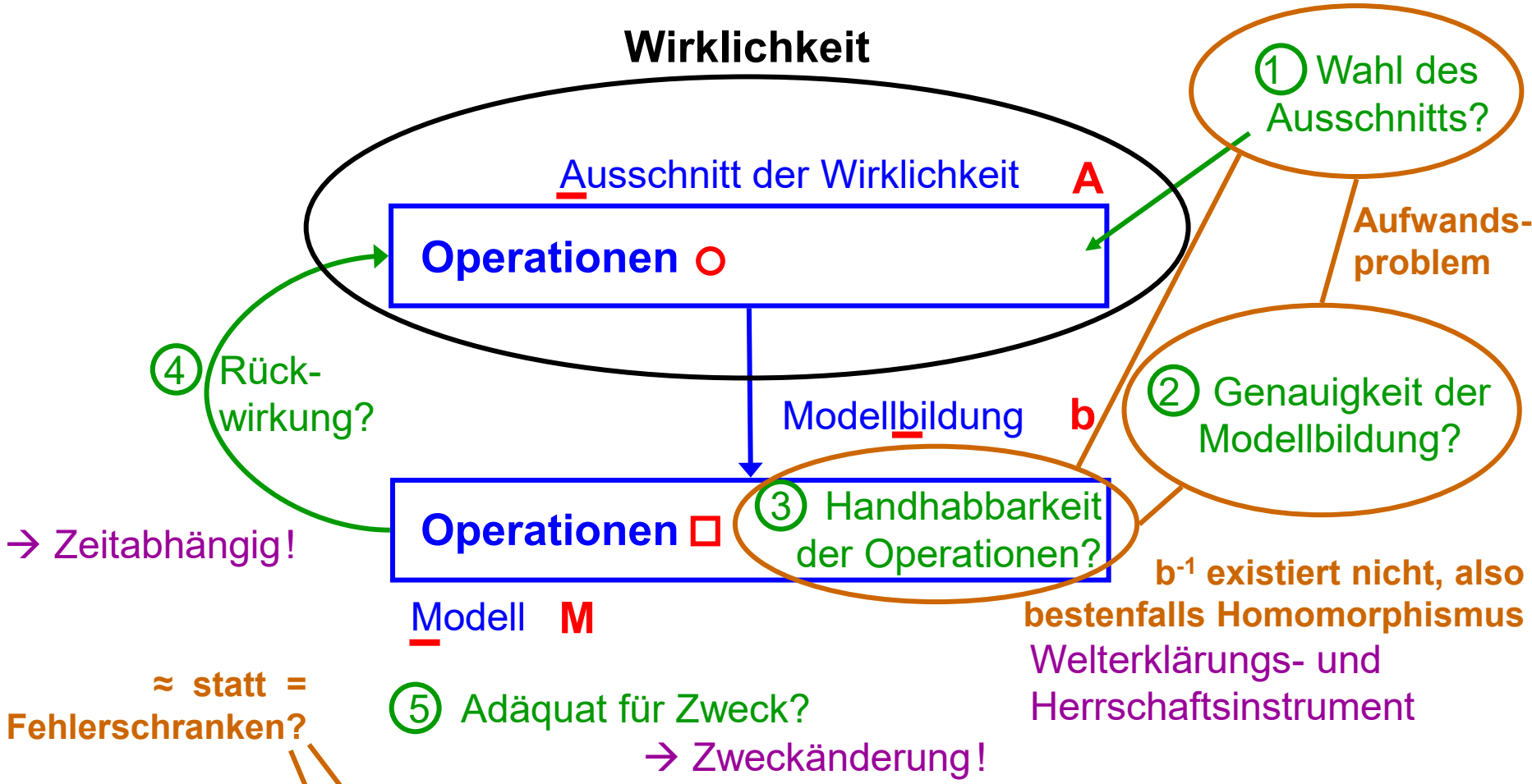
AP/ Knut Christianson/ Nature

Satellitenbild vom Thwaites-Gletscher in der Westantarktis

Fehlerhaftigkeit menschlichen Modellierens und Gestaltens (1)



Fehlerhaftigkeit menschlichen Modellierens und Gestaltens (1)

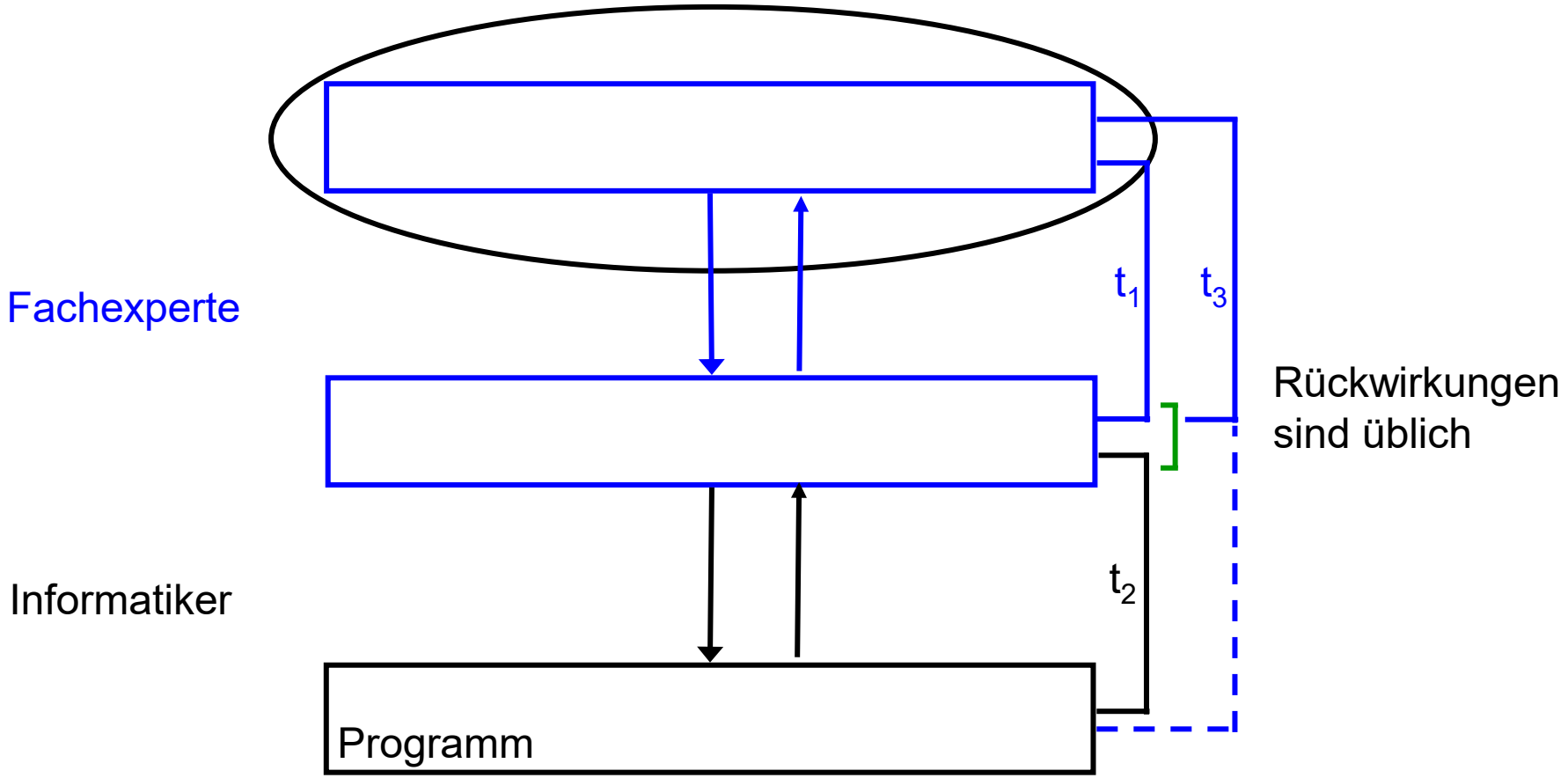


$$\circ\, A = b^{-1}(b(\circ)\, b(A)) \qquad (= b^{-1}(\square\, M))$$

$$b\,(\circ\, A) = b(\circ)\, b(A) \qquad (= \square\, M)$$

b sollte bzgl. aller Operationen ein Isomorphismus sein

Fehlerhaftigkeit menschlichen Modellierens und Gestaltens (2)



$t_1 < t_2 < t_3$ Iteration

öfter miteinander reden

1. Informatiker muss in Anwendungsgebiet Erfahrung haben

2. Fachexperte sollte zumindest etwas Informatik verstehen

Verletzlichkeit der Gesellschaft / Technikfolgenabschätzung

„Die Technikfolgenabschätzung befasst sich mit der Beobachtung und Analyse von Trends in Wissenschaft und Technik und den damit zusammenhängenden gesellschaftlichen Entwicklungen, insbesondere der Abschätzung der Chancen und Risiken. Des Weiteren soll die Technikfolgenabschätzung auch politische Handlungsempfehlungen oder Richtlinien für die Vermeidung von Risiken und die verbesserte Nutzung der Chancen geben…“ [Wikipedia, 11. April 2013]

Technikfolgenabschätzung

Studie: Roboter bedrohe

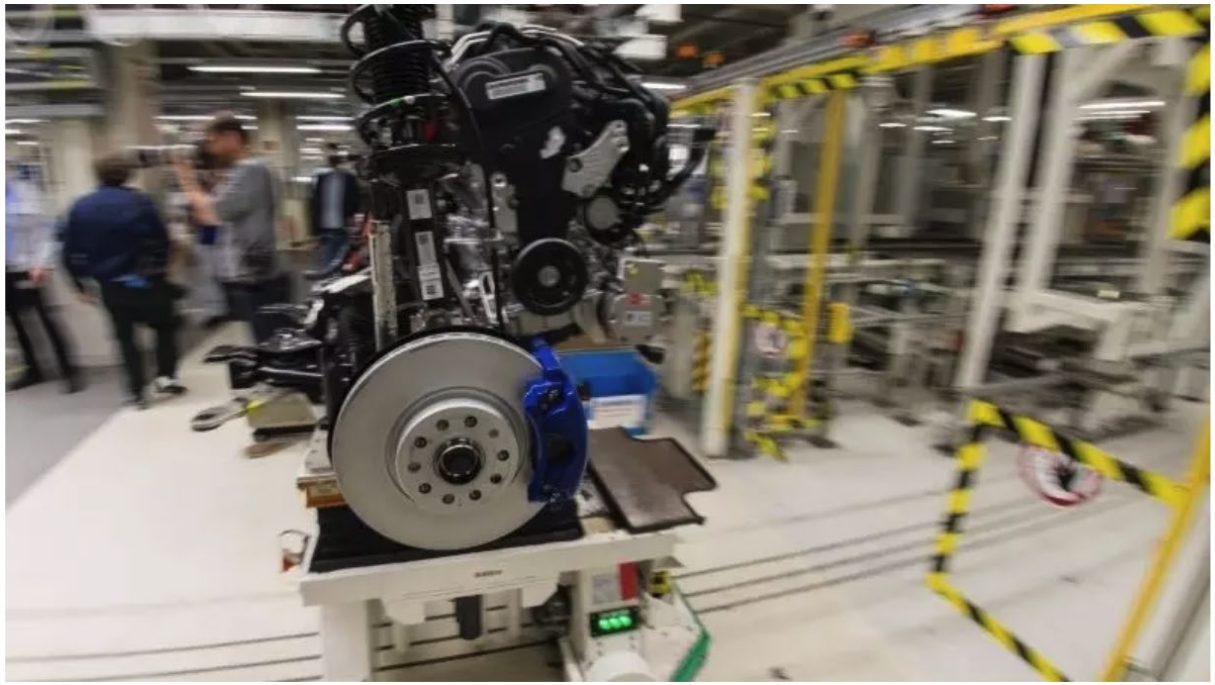
Sicher | https://www.heise.de/newsticker/meldung/Studie-Roboter-bedrohen-Jobs-in-Deutschland-staerker-als-in-anderen-Industrienationen-4012748.html

heise online > News > 04/2018 > Studie: Roboter bedrohen Jobs in Deutschland stärker als in anderen…

Studie: Roboter bedrohen Jobs in Deutschland stärker als in anderen Industrienationen

07.04.2018 16:36 Uhr – Bernd Mewes

vorlesen



Ein Roboter transportiert im VW-Werk in Wolfsburg einen Motorblock mit Radaufhängung. (Bild: dpa, Sebastian Gollnow/Archiv)

Die Entwicklung von Robotern und Software kann in etwa 20 Jahren jeden fünften Arbeitnehmer in Deutschland ersetzen, besagt eine OECD-Studie. Deutschland ist stärker betroffen als die meisten anderen Mitgliedsstaaten.

Technikfolgenabschätzung

Studie: Mehr Jobs durch

Sicher | https://www.heise.de/newsticker/meldung/Studie-Mehr-Jobs-durch-Roboter-und-Digitalisierung-4010846.html

heise online > News > 04/2018 > Studie: Mehr Jobs durch Roboter und Digitalisierung

Studie: Mehr Jobs durch Roboter und Digitalisierung

04.04.2018 17:21 Uhr – Oliver Bünte

vorlesen

(Bild: KUKA)

Ist die Angst vor Arbeitsplatzvernichtung durch den Einsatz von Robotern und fortschreitender Digitalisierung unbegründet? Eine Studie des ZEW kommt zu dem Schluss, dass durch neue Technik mehr Arbeitsplätze geschaffen als vernichtet werden.

Technikfolgenabschätzung — Dilemmas

- nach Collingridge (1980):
  - Technikfolgen lassen sich besser abschätzen / messen je weiter die Technik entwickelt / erprobt / in Anwendung ist
  - Gestaltung / Veränderung von Technik wird um so teurer, je weiter die Entwicklung vorangeschritten ist

- Expertendilemma (Nennen/Garbe 1996):
  - Expertengutachten widersprechen sich oftmals
  - Gutachten / Gegengutachten Problematik
  - Ursache (Grunwald 2010):
    - Unvermeidbarkeit von Bewertungen in Gutachten
    - Trennung von wertfreiem „Erkennen“ von Technikfolgen und *anschließender* Bewertung nicht möglich
      - „Erkennen“ hängt von Bewertung ab

Verletzlichkeit der Gesellschaft / Technikfolgenabschätzung

- Literatur:
  - Armin Grunwald: „Technikfolgenabschätzung - eine Einführung“, Edition Sigma, 2010
  - Alexander Roßnagel et al. : „Die Verletzlichkeit der ‚Informationsgesellschaft‘ “, Sozialverträgliche Technikgestaltung, Band 5, Westdeutscher Verlag, 1990.
    Online: http://nbn-resolving.de/urn:nbn:de:hebis:34-2009103030803
  - Literatursammlung der Projektgruppe verfassungsverträgliche Technikgestaltung e. V. (www.provet.org)

Informatik und Gesellschaft?

Schadensarten

- Einzelschäden
  - ggf. unabhängig vom IuK Einsatz
  - teilweise verhinderbar durch IuK Einsatz („Risiko Mensch“)
  - Gefahr: hohe Einzelschäden, beispielsweise durch Datenverlust
- Kumulationsschaden
  - IuK Technik erleichtert schädliche Handlungen, die *vielfach und unabhängig* voneinander ausgeführt werden
    - Beispiele (vermutlich): SPAM, Phising, Cyber-Angriffe
- Multiplikationsschaden
  - dieselbe IuK Technik wird von vielen (parallel) benutzt
  - geringer Einzelschaden → hoher Gesamtschaden
- Kopplungsschaden
  - gleichzeitiges Auftreten von Schäden in *scheinbar* entkoppelten Systemen
  - Problem: fehlende Diversität, beispielsweise Monokultur bei Betriebssystemen, Hardware, Entwurfswerkzeugen etc.
- Komplexschaden
  - große Schadensauswirkung durch Vernetzung von (IuK) Systemen
  - Beispiel: „Blackout“ in der Stromversorgung durch gekoppelte Regelkreise

Risiko

- Risiko bezüglich eines Ereignisses, Schadens etc.:

Eintrittswahrscheinlichkeit • Schadensausmaß

- Probleme:
  - Eintrittswahrscheinlichkeiten:
    - Erfahrungswissen bei IuK Technik / Systemen oftmals nicht vorhanden
    - Verständnisproblem: Unwahrscheinlich vs. Unmöglich
  - Schadensausmaß
    - in komplexen IuK System oftmals schwer zu bestimmen
    - Daten oftmals nicht veröffentlicht

Zehn Thesen zur Verletzlichkeit der „Informationsgesellschaft“

[Roßnagel et al., 1989]

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.
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.
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.

Technologie & Gesellschaft

- **“Visions of Technology”,** Texte von Daniela Cerqui aus FIDIS D12.2, **http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-d12.2_Study_on_Emerging_AmI_Technologies.pdf**
- **Technological neutralism:** technology is neutral, and only its use can be good or bad. The user is the only responsible person for the good or bad result. The only thing we can do is to promote good uses.
- **Technological determinism:** technology is intrinsically either good or bad.
  - **technophile determinism**: technology is the right solution for solving all the problems of the world (knowledge, wealth, and even happiness for everyone).
  - **technophobe determinism**: technology will lead us to a huge catastrophe.

Rebound-Effekt

- Ziel:
  - Einsparung von Ressourcen (beispielsweise Energie) durch Effizienzsteigerung

- Rebound-Effekte:
  - Direkter Rebound-Effekt: gesenkte „Kosten“ (=Ressourcenverbrauch) → billiger → mehr Nachfrage → Gesamtkosten steigen
  - Indirekter Rebound-Effekt: gesenkte „Kosten“ → mehr „Ressourcen“ für anderes → Gesamtkosten steigen
  - Makroökonomischer Rebound-Effekt: gesenkte „Kosten“ → Verbilligung von Produkten → mehr Nachfrage → Gesamtkosten steigen

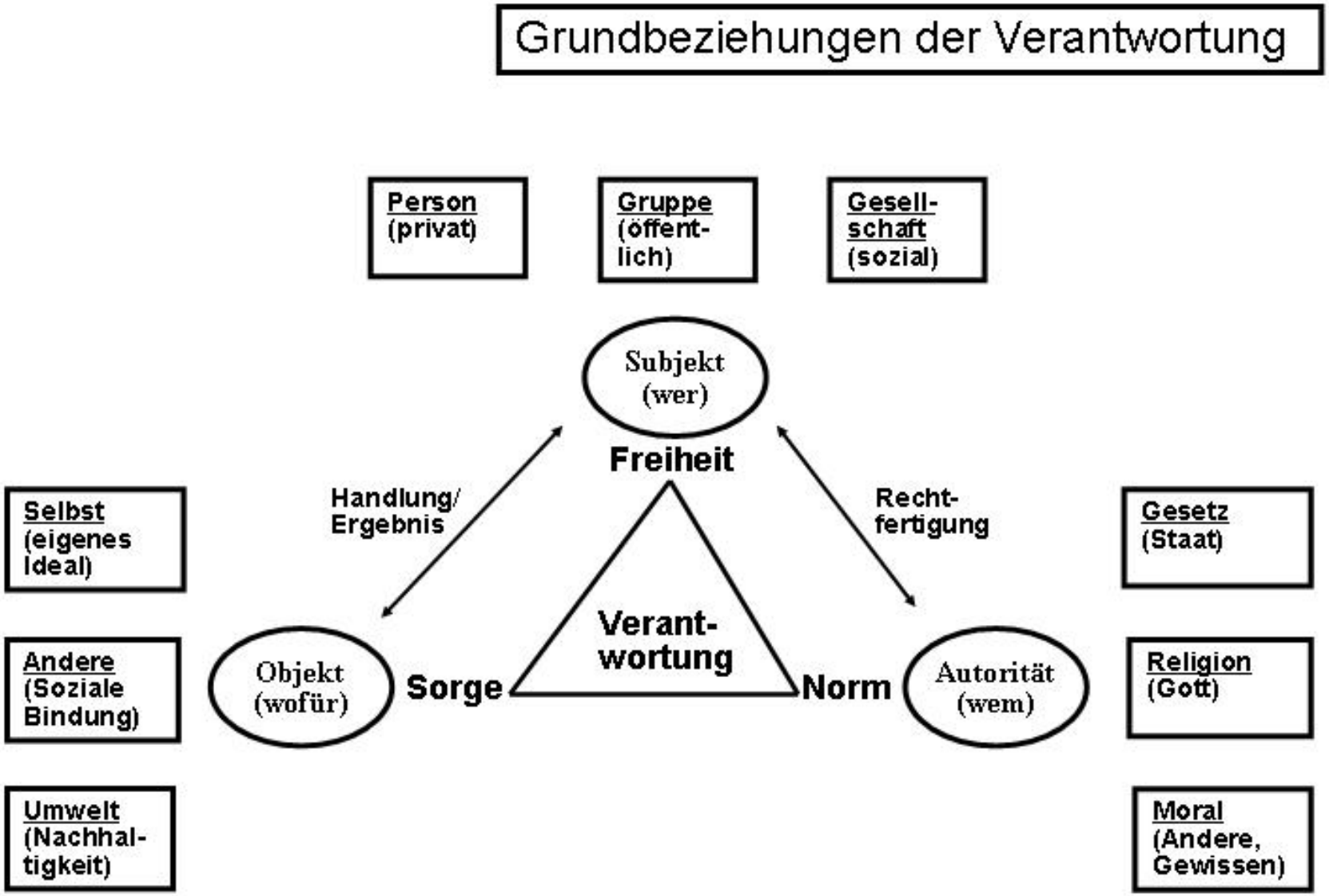
Rebound-Effekt

- Ursachen:
  - Finanzielle Einsparungen: → mehr Konsum
  - Transformations-Effekt: Effizienzsteigerungen → geändertes Konsumverhalten & gesellschaftliche Transformationen → negative Effekte mit Steigerung des Gesamtressourcenverbrauchs
  - Mentaler Rebound-Effekt: gesenkter Ressourcenverbrauch → „Gutes Gewissen“ → mehr Konsum
- Lösungsansätze
  - künstliche Verteuerung → Steuern
  - Gesamtressourcenverbrauch reglementieren

Ethik & Verantwortung

- Verantwortung:
  - vielfältig diskutiertes Konzept
  - dreistellige Grundrelation: *Jemand* ist für *etwas* gegenüber *jemandem* verantwortlich
  - Voraussetzung: **Handlungsfreiheit**
  - „Zuschreibung einer Pflicht zu einer handelnden Person … gegenüber einer anderen Person … aufgrund eines normativen Anspruchs, der durch eine Instanz eingefordert werden kann und vor dieser zu rechtfertigen … ist “ [Wikipedia, 11. April 2013]

Ethik & Verantwortung



[aus Wikipedia, Artikel Verantwortung, Auto: Lutz Hartmann]

Ethik & Verantwortung

- Verantwortung:
  - vielfältig diskutiertes Konzept
  - dreistellige Grundrelation: *Jemand* ist für *etwas* gegenüber *jemandem* verantwortlich
  - Voraussetzung: **Handlungsfreiheit**
  - „Zuschreibung einer Pflicht zu einer handelnden Person … gegenüber einer anderen Person … aufgrund eines normativen Anspruchs, der durch eine Instanz eingefordert werden kann und vor dieser zu rechtfertigen … ist “ [Wikipedia, 11. April 2013]
- Ethik:
  - Teilgebiete der Philosophie
  - befaßt sich mit Moral, insbesondere hinsichtlich ihrer Begründbarkeit
    - Moral: faktisches und erwartetes (richtiges) Handeln von Menschen

Teller über die Verantwortung des Wissenschaftlers

- Edward Teller = „Vater der Wasserstoffbombe “
- Zeit-Artikel: „*Bloß keine Selbstzweifel*“, 28. April 1995, http://www.zeit.de/1995/18/Bloss_keine_Selbstzweifel
- **Pflicht des Wissenschaftlers** = Wissen produzieren und dessen technische Umsetzung ermöglichen – ohne Beschränkung und unter allen Umständen
- **konkrete Anwendung, Verantwortung** = Sache politischer Entscheidung; Erkenntnisse sind nicht moralischer Natur

- *Physiker von Los Alamos haben Bombe nicht gemacht, sondern „gefunden“*

Roboter-Gesetze

aus Issac Asimov „Runaround“ (März 1942)

1. Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit (wissentlich) zulassen, dass einem menschlichen Wesen Schaden zugefügt wird.

2. Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren.

3. Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert.

Roboter-Gesetze

Isaac Asimiov „The Evitable Conflict“ (Juni 1950)

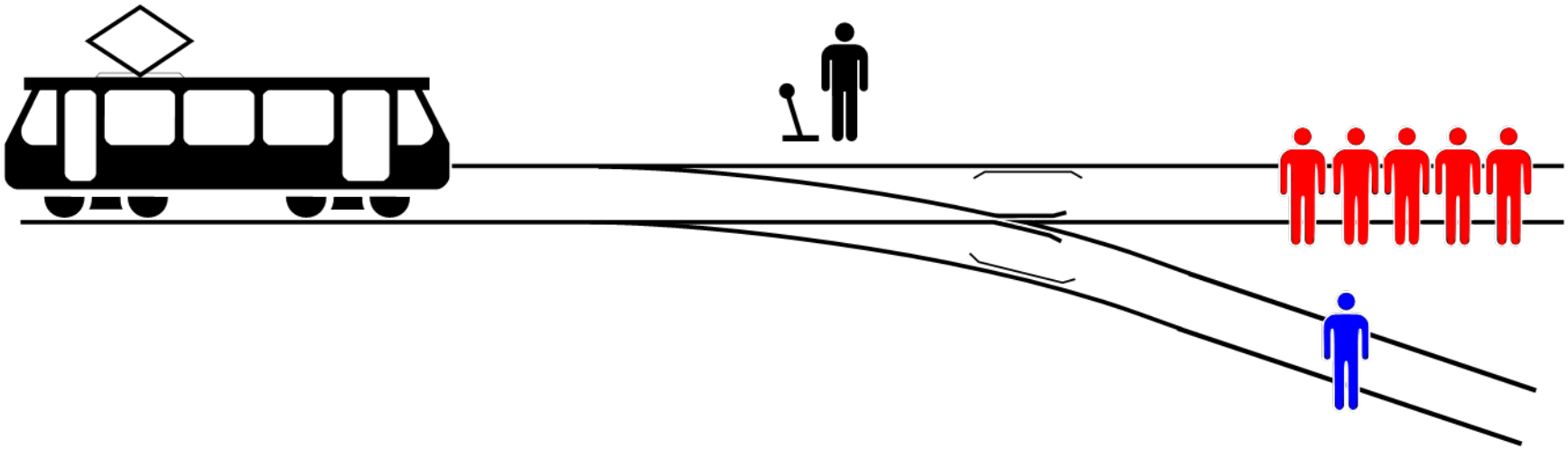
0. Ein Roboter darf die Menschheit nicht verletzen oder durch Passivität zulassen, dass die Menschheit zu Schaden kommt.

1. Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit (wissentlich) zulassen, dass einem menschlichen Wesen Schaden zugefügt wird, außer er verstieße damit gegen das nullte Gesetz.

2. Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren.

3. Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert.

Das Trolley Problem –
ethisches Dilemma beim autonomen Fahren



[https://de.wikipedia.org/wiki/Trolley-Problem#/media/Datei:Trolley_Problem.svg]

„Es kann sein, daß ein Weichensteller, um einen drohenden Zusammenstoß zu verhindern, der aller Voraussicht nach sehr viele Menschenleben kosten wird, den Zug so leitet, daß zwar auch Menschenleben aufs Spiel gesetzt werden, aber sehr viel weniger, als wenn er den Dingen ihren Lauf ließe.“

[Karl Engisch: *Untersuchungen über Vorsatz und Fahrlässigkeit im Strafrecht*. O. Liebermann, Berlin 1930]

Merke: Abwägung von Leben gegeneinander widerspricht dem deutschen Grundgesetz!

Gesellschaft für Informatik e.V. (GI)

- gegründet 1969 in Bonn
- ca. 24000 Mitglieder
- Tätigkeitsfeld:
  - Unterstützung der fachlichen und beruflichen Arbeit von Informatikern und Informatikerinnen
  - **Herausgabe** und Förderung **von Fachpublikationen**
  - **Mitwirkung** im Vorfeld politischer Planung und Gesetzgebung zur Forschungs-, Bildungs- und Technologiepolitik
  - Abgabe von **öffentlichen** Empfehlungen und **Stellungnahmen** zur Informatik
  - **Förderung des wissenschaftlichen Nachwuchses** und Ausrichtung von Informatik-Wettbewerben
  - **Förderung von** in der Informatik tätigen **Frauen** mit dem Ziel ihrer faktischen Gleichstellung
  - **Bereitstellung fachlicher Kommunikationsforen** durch Veranstaltung von Arbeitstreffen, Fachtagungen, Kongressen und Ausstellungen
  - **Mitwirkung** im Bereich von Normen, Standards und Validierungen
  - **Zusammenarbeit** mit nationalen und internationalen Vereinigungen

GI Ethik Leitlinien

- verabschiedet am 13.01.1994 vom Präsidium der GI
- bestätigt am 16.12.1994 von den Mitgliedern
- überarbeitete Version am 29. Januar 2004 durch GI-Präsidium angenommen, erneut überarbeitet am 29. Juni 2018
- „*Der offene Charakter der nachfolgenden Artikel wird mit dem Begriff Leitlinien unterstrichen.*“
- https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien

GI Ethik Leitlinien (Version 2004)

- berufsethische Konflikte Gegenstand gemeinsamen Nachdenkens und Handelns
- **Fachkompetenz** nach dem Stand von Wissenschaft und Technik ständig verbessern
- **Auswirkungen** von Informatiksystemen **beurteilen** und geeignete Lösungen vorschlagen
- **Rechte** und Interessen der verschiedenen **Betroffenen** verstehen und **berücksichtigen**
- einschlägige **rechtliche Regelungen** kennen, **einhalten** und an ihrer Fortschreibung mitwirken
- **Urteilsfähigkeit entwickeln**, um eigenes und gemeinschaftliches Handeln in Beziehung zu gesellschaftlichen Fragestellungen zu setzen und zu bewerten

GI Ethik Leitlinien (Version 2004)

- in Situationen, in denen Pflichten gegenüber Arbeitgebern oder Kundenorganisationen **in Konflikt** mit der Verantwortung gegenüber anderweitig Betroffenen stehen **mit Zivilcourage handeln**
- Einsatz von Informatiksystemen zur **Verbesserung der lokalen und globalen Lebensbedingungen**
- **Verantwortung für soziale und gesellschaftliche Auswirkungen** der eigenen Arbeit
- **Einfluß nehmen auf** Positionierung, Vermarktung und Weiterentwicklung von Informatiksystemen zu ihrer **sozial verträglichen Verwendung**
- **interdisziplinäre Diskurse** zu ethischen und sozialen Problemen der Informatik initiieren und **fördern**

GI Ethik Leitlinien (Version 2004)

- Informatiker in Führungsposition:
  - Weiterbildung ermöglichen
  - aktiv für Diskussion eintreten bezüglich Übernahme individueller und gemeinschaftlicher Verantwortung
  - bei Einführung von Informatiksystemen Betroffene an der Gestaltung der Systeme und ihrer Nutzungsbedingungen angemessen beteiligen
  - keine Kontroll- und Überwachungstechniken ohne Unterrichtung und Beteiligung der Betroffenen zulassen

- Informatiker in Lehre & Forschung:
  - **Lernende auf deren individuelle und gemeinschaftliche Verantwortung vorbereiten und selbst hierbei Vorbild sein**
  - Regeln des guten wissenschaftlichen Arbeitens einhalten

Google-Mitarbeiter prote
Sicher | https://www.heise.de/newsticker/meldung/Google-Mitarbeiter-protestieren-gegen-Beteiligung-an-Militaer-Projekt-4011328.html

Google-Mitarbeiter protestieren gegen Beteiligung an Militär-Projekt

05.04.2018 11:40 Uhr – Andreas Wilkens

vorlesen

Blick in das Combined Air Operations Center der Al Udeid Air Base der US-Luftwaffe in Katar. (Bild: US Air Force)

Google ist an einem Projekt des US-Verteidigungsministerium beteiligt, in dem es um die automatische Auswertung von Drohnen-Aufnahmen geht. Dagegen wehren sich tausende Mitarbeiter.

Gut 3100 Google-Mitarbeiter haben einen offenen Brief an ihren Chef Sundar Pichai unterschrieben, in dem sie gegen die Beteiligung ihres Unternehmens an dem seit 2017 laufenden Project Maven des US-amerikanischen Verteidigungsministeriums protestieren.

GI Ethik Leitlinien (Version 2018)

- **Art. 1 Fachkompetenz**
  - Ständige Verbesserung der Fachkompetenz
  - kritisiert den Stand von Wissenschaft und Technik konstruktiv
- **Art. 2 Sachkompetenz und kommunikative Kompetenz**
  - Auswirkungen von IT-Systemen im Anwendungsumfeld beurteilen und geeignete Lösungen vorschlagen können
  - Rechte, Bedürfnisse und Interessen der Betroffenen verstehen und berücksichtigen
- **Art. 3 Juristische Kompetenz**
  - Mitwirkung an der Gestaltung rechtlicher Regelungen
- **Art. 4 Urteilsfähigkeit**
  - eigenes und gemeinschaftliches Handeln kritisch hinterfragen
  - Grenzen der eigenen Urteilsfähigkeit erkennen

GI Ethik Leitlinien (Version 2018)

- **Art. 5 Arbeitsbedingungen**
  - Einsatz für sozial verträgliche Arbeitsbedingungen mit Weiterbildungs- und Gestaltungsmöglichkeiten
- **Art. 6 Organisationsstrukturen**
  - Übernahme individueller und gemeinschaftlicher Verantwortung fördern
- **Art. 7 Lehren und Lernen**
  - Fähigkeit zum kritischen Denken fördern
  - Vorbereiten auf individuelle und gemeinschaftliche Verantwortung
  - *Das GI-Mitglied, das in Schule, Hochschule oder Weiterbildung Informatik lernt, fordert dies von den Lehrenden ein.*
- **Art. 8 Forschung**
  - Offenheit und Transparenz
  - Fähigkeit zur Äußerung und Akzeptanz von Kritik
  - Auswirkungen der eigenen wissenschaftlichen Arbeit thematisieren
  - Grenzen verständlich machen

GI Ethik Leitlinien (Version 2018)

- **Art. 9 Zivilcourage**
  - Schutz und Wahrung der Menschenwürde
  - auch in Situationen, in denen Pflichten gegenüber Auftraggebenden in Konflikt mit der Verantwortung gegenüber Anderen stehen
  - kann in begründeten Ausnahmefällen den öffentlichen Hinweis auf Missstände einschließen
- **Art. 10 Soziale Verantwortung**
  - mit IT-Systemen zur Verbesserung der Lebensbedingungen beitragen
  - Verantwortung für soziale und gesellschaftliche Auswirkungen
  - Einfluss nehmen auf sozial verträgliche und nachhaltige Verwendung von IT-Systemen
- **Art. 11 Ermöglichung der Selbstbestimmung**
  - Betroffene an Gestaltung und Nutzungsbedingungen von IT-Systemen angemessen beteiligen

FIfF e.V. — Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

- gegründet 1984
- ca. 700 Mitglieder, hauptsächlich Fachleute aus dem Bereich Informatik
- Berufsverband, der Informationstechnik kritisch begleitet

FIfF e.V. — Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

- Ziele: (http://www.fiff.de/about)
  - warnen wir die Öffentlichkeit vor Entwicklungen in unserem Fachgebiet, die wir für schädlich halten;
  - setzen wir möglichen Gefahren eigene Vorstellungen entgegen;
  - kämpfen wir gegen den Einsatz der Informationstechnik zur Kontrolle und Überwachung;
  - engagieren wir uns für eine Abrüstung der Informatik in militärischen Anwendungen;
  - fördern wir die Entwicklung von ökologisch verträglichen Wirtschaftskreisläufen mit Hilfe von Informationstechnik;
  - unterstützen wir die menschengerechte Gestaltung von Arbeitsprozessen;
  - setzen wir uns bei Gestaltung und Nutzung der Informationstechnik für die Gleichberechtigung von Menschen mit Behinderungen ein;
  - arbeiten wir gegen die Benachteiligung von Frauen in der Informatik;
  - wehren wir uns gegen jegliche rassistische und sexistische Nutzung oder andere diskriminierende Nutzung der Informationstechnik;
  - setzen wir der Vorherrschaft der Ökonomie eine humane und ökologische Orientierung entgegen.

Association for Computing Machinery (ACM)

- gegründet 1947
- weltweite Informatikervereinigung
- mehr als 100 000 Mitglieder

ACM Code of Ethics and Professional Conduct

- aktuelle Version vom 22. Juni 2018
- https://acm.org/code-of-ethics
- GENERAL MORAL IMPERATIVES
  - Contribute to society and human well-being
  - Avoid harm to others
  - Be honest and trustworthy
  - Be fair and take action not to discriminate
  - Respect the work required to produce new ideas, inventions, creative works, and computing artifacts
  - Respect the privacy of others
  - Honor confidentiality

ACM Code of Ethics and Professional Conduct

- MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES
  - Strive to achieve high quality in both the processes and products of professional work
  - Maintain high standards of professional competence, conduct, and ethical practice
  - Know and respect existing rules pertaining to professional work
  - Accept and provide appropriate professional review
  - Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks
  - Perform work only in areas of competence.
  - Foster public awareness and understanding of computing, related technologies, and their consequences
  - Access computing and communication resources only when authorized or when compelled by the public good
  - Design and implement systems that are robustly and usably secure

ACM Code of Ethics and Professional Conduct

- ORGANIZATIONAL LEADERSHIP IMPERATIVES
  - Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities
  - Manage personnel and resources to design and build information systems that enhance the quality of working life
  - Acknowledge and support proper and authorized uses of an organization's computing and communication resources
  - 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
  - Articulate and support policies that protect the dignity of users and others affected by a computing system
  - Create opportunities for members of the organization to learn the principles and limitations of computer systems

Neugestaltet 2018

ACM Code of Ethics and Professional Conduct

- PROFESSIONAL LEADERSHIP PRINCIPLES
- LEADER = any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities
  - Ensure that the public good is the central concern during all professional computing work
  - Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group
  - Manage personnel and resources to enhance the quality of working life
  - Articulate, apply, and support policies and processes that reflect the principles of the Code
  - Create opportunities for members of the organization or group to grow as professionals
  - Use care when modifying or retiring systems
  - Recognize and take special care of systems that become integrated into the infrastructure of society

Paketmanager npm: Entwickler m

https://www.heise.de/news/Paketmanager-npm-Entwickler-macht-eigene-Packages-unbrauchbar-6322366.html

Paketmanager npm: Entwickler macht eigene Packages unbrauchbar

Die manipulierten Pakete sollen offensichtlich eine Botschaft an Großunternehmen sein, die Open Source nutzen, ohne die Developer zu bezahlen.

Lesezeit: **4 Min.** In Pocket speichern 573

ACM Code of Ethics and Professional Conduct

- COMPLIANCE WITH THE CODE
  - Uphold, promote, and respect the principles of the Code
  - Treat violations of this code as inconsistent with membership in the ACM

Institute of Electrical and Electronics Engineers (IEEE)

- internationaler Verband von Ingenieuren (hauptsächlich Elektrotechnik / Informationstechnik)
- Wurzeln reichen zurück bis 1884
- mehr als 400000 Mitglieder
- mehr als 160 Länder
- seit 1963: „IEEE Code of Ethics“
- Juni 2014 „IEEE Code of Conduct“

IEEE Code of Ethics

- accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment
- avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist
- be honest and realistic in stating claims or estimates based on available data;
- reject bribery in all its forms
- improve the understanding of technology; its appropriate application, and potential consequences
- 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
- seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others
- treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin
- avoid injuring others, their property, reputation, or employment by false or malicious action
- assist colleagues and co-workers in their professional development and to support them in following this code of ethics

IEEE Code of Conduct

- Be respectful of others
  - We will be respectful of the privacy of others and the protection of their personal information and data.
- Treat people fairly
- Avoid injuring others, their property, reputation or employment
- Comply with applicable laws in all countries where IEEE does business and with the IEEE policies and procedures

International Federation for Information Processing (IFIP)

- Dachorganisation von Informatikervereinigungen
  - aus mehr als 56 Ländern
  - aus allen 5 Kontinenten
  - mit mehr als 500000 Mitgliedern
- gegründet 1960 unter Schirmherrschaft der UNESCO
  - im Ergebnis des ersten World Computer Congress (Paris, 1959)
- Status: internationale Nichtregierungsorganisation
  - offiziell anerkannt und eingetragen in Österreich
- Publikation: „Ethics of Computing: Codes, spaces for discussion and law“
  - Analyse von 30 nationalen Ethik-Richtlinien
- Status der „IFIP International Code of Ethics“ ??

A. Pfitzmann: „Zur Verantwortung der Informatiker“

[Datenschutz-Berater 15/8-9 (August 1991), Seiten: 2-7]

- für jedes (Sub-)System durch Dokumentation **Systemtyp festlegen** (präzise definiert, vage definiert, sozio-technisch etc.)
- nur (Sub-)Systeme entwerfen, produzieren, betreiben, verbinden oder modifizieren, nachdem alle **Schnittstellen vollständig verstanden** sind
- für jedes entworfene, produzierte, betriebene, verbundene oder modifizierte (Sub-)System *S* **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**.“

A. Pfitzmann: „Zur Verantwortung der Informatiker“

- **volle persönliche Verantwortung** übernehmen für unterschriebene Erklärungen (inklusive strafrechtlichen oder zivilrechtlichen Konsequenzen)
- bei Konstruktion von größeren Systemen aus Subsystemen
  - **Zusicherungen** von Eigenschaften der verwendeten Subsysteme auf Plausibilität und Glaubwürdigkeit **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?
  - im Zweifelsfall defensiv vorgehen:
    - auf unklares Subsystem verzichten
    - zugesicherte Leistungen nicht ausreizen
- für Innovation und Experimentieren
  - IT-Systeme möglich, die nicht nach obigen Grundsätzen entwickelt wurden
  - wichtig: Kennzeichnung und Einsatz nur mit Zustimmung aller Betroffenen

Rangfolge von Gesetzen

1. **geographischer** Bereich
   - nicht immer eindeutig zu bestimmen; insbesondere im Bereich „Internet“:
     - *Herkunftslandprinzip*: Recht des Landes des Anbieters einer Ware / Dienstleistung
     - *Bestimmungslandprinzip:* Recht des Landes in das die Ware / Dienstleistung geliefert wird (vor allem im Steuerrecht)

Rangfolge von Gesetzen

2. Regelungen **übergeordneter** Organe gehen vor Regelungen untergeordneter Organe
   - *lex superior derogat legi inferiori*

1. Verfassung
2. Gesetze
3. Rechtsverordnungen
4. Verwaltungsvorschriften

1. EU-Recht
2. Bundesrecht
3. Landesrecht

Rangfolge von Gesetzen

3. **speziellere** Regelung geht vor allgemeiner Regelung
   - *lex specialis derogat legi generali*
   - Beispiel: Datenschutz; allgemein geregelt im Bundesdatenschutzgesetz (BDSG); spezielle Regelungen in über 150 Spezialgesetzen, etwa Sozialgesetzbuch (SGB)

4. **neuere** Regelungen gehen vor älteren Regelungen
   - *lex posterior derogat legi priori*

EU-Recht

- EG-/EU-Verordnung (engl.: Regulation)
  - erlassen gemeinsam vom Rat der Europäischen Union und dem Europäischen Parlament
  - gelten unmittelbar in allen Mitgliedsstaaten
- EG-/EU-Richtlinie (engl.: Directive)
  - erlassen gemeinsam vom Rat der Europäischen Union und dem Europäischen Parlament
  - enthalten in der Regel eine Umsetzungsfrist
  - kann nach Ablauf der Frist unmittelbare Wirkung entfalten

Probleme für Nicht-Juristen

§ 113b TKG:

Der nach § 113a Verpflichtete **darf** die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten

- zur Verfolgung von Straftaten,
- zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder
- zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

an die zuständigen Stellen auf deren Verlangen übermitteln…

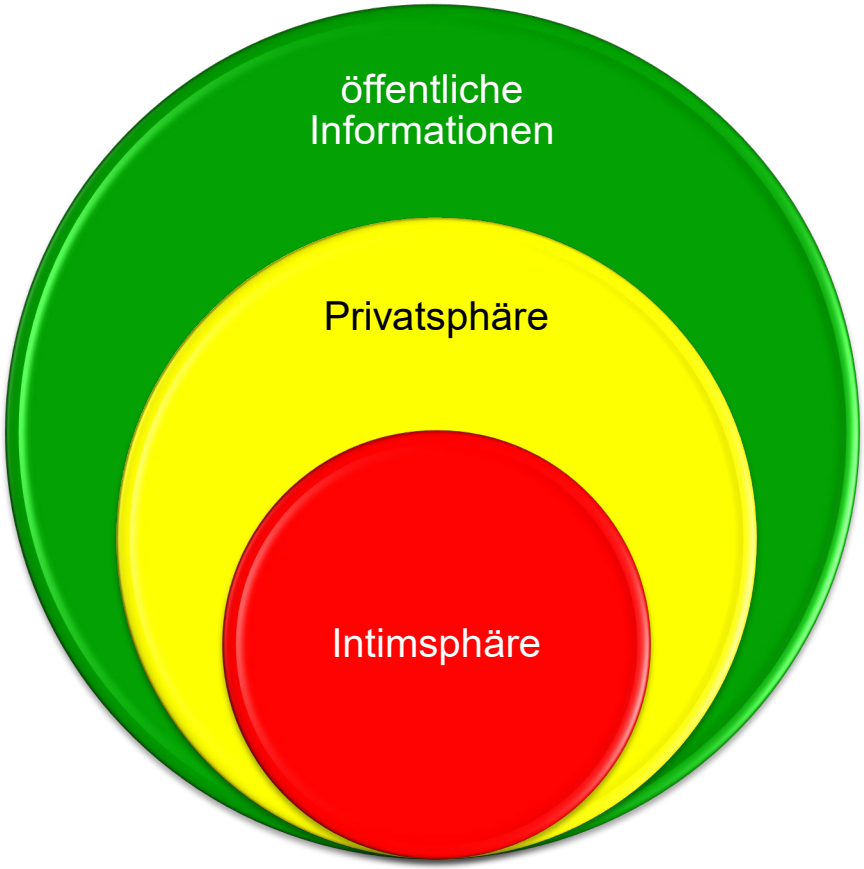
➔ § 100g StPO enthielt Verpflichtung zur Herausgabe von Daten
stark vereinfacht: *alles was man herausgeben darf, muß man auch herausgeben*

Datenschutz vs. Datensicherheit

- keine wirklich klaren Definitionen / Abgrenzungen vorhanden
- Datenschutz:
  - Schutz ***vor*** Daten
- Datensicherheit
  - Schutz ***von*** Daten

Datenschutzmodelle

- Sphärenmodell
  - unterschiedliche Attribute / Daten besitzen unterschiedliche Schutzwürdigkeit
  - Problem:
    - Zuordnung von Attributen abhängig von persönlicher Einstellung, Sozialisierung, Umfeld, Kultur etc.
      - Beispiel: (N)aktfoto



Datenschutzmodelle

- Rollenmodell
  - Schutzwürdigkeit richtet sich nach der Rolle des Kommunikationspartners
    - Beispiel: Übermittlung medizinischer Daten an Hausarzt vs. Veröffentlichung im Internet
  - Problem:
    - Verkettung: unterschiedliche Rollen werden von der selben Person eingenommen
    - Benutzbarkeit

Datenschutzmodelle

- Mosaikmodell
  - alle Daten sind schutzwürdig → wertvolle Mosaiksteine
  - konkreter Mißbrauch von Daten ergibt sich erst durch Verkettungsmöglichkeiten
  - Beispiel (fiktiv):
    - Schuhgröße, Vorname, Postleitzahl, Geschlecht identifiziert Person eindeutig
  - Problem:
    - jegliche Datenpreisgabe müßte vermieden werden
    - Verkettung muß verhindert werden

[Quelle: Wikipedia]

Recht auf "informationelle Selbstbestimmung"

⌘ Volkszählungs-Urteil (BVerfGE 65,1 - 15. Dezember 1983)

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem ***Recht auf informationelle Selbstbestimmung*** *wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."*

„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren "

Datenschutzprinzipien

- Datensparsamkeit
- Datenminimierung
- Datenvermeidung
- Verhältnismäßigkeit
- Zweckbindung
- Transparenz
- Zustimmung
- Auskunftsrecht
- Recht auf Löschung und Berichtigung
- besonders geschützte Daten

Mosaikmodell

Rollenmodell

Sphärenmodell

Rechtliche Regelungen

- EG-Richtlinien
  - Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie)

    ➔ **Neuregelung 2011 geplant!**

    ➔ **2016 umgesetzt**

    ➔ **gültig seit 25. Mai 2018**
  - Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation
- Bundesdatenschutzgesetz
  - erste Fassung: 1977
  - Neufassung: 2003
  - Letzte Änderung: 2019
- Landesdatenschutzgesetze
  - weltweit erstes Datenschutzgesetz in Hessen 1970
- Spezialgesetze
  - Telemediengesetz

Datenschutzrichtlinie 95/46/EG

- Anwendungsbereich:

  „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.“ [Artikel 3]

  – Ausnahme: rein private / familiäre Datenverarbeitung

- Regelungsgegenstand:

  – Verarbeitung *personenbezogener Daten*

  ➔ „Informationen über eine bestimmte oder bestimmbare natürliche Person “ [Artikel 2]

Datenschutzrichtlinie 95/46/EG

- Grundsätze [Artikel 6]

„Die Mitgliedstaaten sehen vor, daß personenbezogene Daten

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden.

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; … nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden;

e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, … aufbewahrt werden“

Datenschutzrichtlinie 95/46/EG

- Verbot mit Erlaubnisvorbehalt [Artikel 7]

„Die Mitgliedstaaten sehen vor, daß die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn …

a) Die betroffene Person hat ohne jeden Zweifel ihre **Einwilligung** gegeben;

b) erforderlich für die Erfüllung eines Vertrags,

c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

d) erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person

e) erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt

f) erforderlich zur Verwirklichung des berechtigten Interesses, … von … den Dritten …, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, … , überwiegen.“

Datenschutzrichtlinie 95/46/EG

- Besonders schützenswerte Daten [Artikel 8]

„Die Mitgliedstaaten 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.“

- ➔ Verarbeitung jedoch unter bestimmten Umständen möglich; insbesondere:
  - Einwilligung

Datenschutzrichtlinie 95/46/EG

- Informationsrecht [Artikel 10, 11]
  - Identität des für die Verarbeitung Verantwortlichen
  - Zweckbestimmungen
  - Empfänger der Daten
- Auskunftsrecht [Artikel 12]
- Widerspruchsrecht [Artikel 14]
- Automatisierte Einzelentscheidungen zum Zwecke der Bewertung einzelner Aspekte einer Person wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens sind unzulässig [Artikel 15]

Datenschutzrichtlinie 95/46/EG

- Meldepflicht und Vorabkontrolle vor Verarbeitung personenbezogener Daten [Artikel 18, 19, 20]
- Übermittlung personenbezogener Daten in ein Drittland nur zulässig, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet [Artikel 25]
- öffentliche Kontrollstelle für den Datenschutz [Artikel 28]
  - völlige Unabhängigkeit
  - Untersuchungsbefugnisse, wirksame Einwirkungsbefugnisse, Klagerecht
- europäische Datenschutzgruppe [Artikel 29, Artikel 30]
  - Article 29 Working Party
  - unabhängig
  - umfangreiche beratende und überwachende Funktion zu allen Fragen des Datenschutzes
  - 1 Vertreter pro Mitgliedsstaat + 1 Vertreter der EU-Kommission + 1 Vertreter der EU-Datenschutzbehörde

Datenschutz-Grundverordnung

- *„VERORDNUNG (EU) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“*
  - angenommen durch EU-Parlament am 14. April 2016
- veröffentlicht: 5. Mai 2016 (L 119/1)
- Inkrafttreten: 5. Mai 2016 + 20 Tage = 25. Mai 2016
- Gültigkeit: 25. Mai 2016 + 2 Jahre = **25. Mai 2018**
- Neuerungen / Besonderheiten:
  - Artikel 17 „Recht auf Löschung ("Recht auf Vergessenwerden") “
  - Artikel 20 „Recht auf Datenübertragbarkeit “
    - Vermeidung von „Lock-in“ Effekten
  - Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“
  - Artikel 33 „Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“
    - ggf. einschließlich Benachrichtigung der Betroffenen
  - Artikel 33 „Datenschutz-Folgenabschätzung“
  - Artikel 77 „Recht auf Beschwerde bei einer Aufsichtsbehörde “
    - „One-Stop-Shop“

Bundesdatenschutzgesetz

- Verpflichtete:
  - öffentliche Stellen des Bundes
  - öffentliche Stellen der Länder (falls keine Regelungen im Landesdatenschutzgesetz)
  - nicht-öffentliche Stellen
    - natürliche und juristische Personen
    - Ausnahme: rein private / familiäre Datenverarbeitung

- Regelungsgegenstand:
  - Verarbeitung *personenbezogener Daten*
  - *„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder* ***bestimmbaren natürlichen*** *Person (Betroffener). “* [§ 3 (1) BDSG]

Bundesdatenschutzgesetz

- Grundprinzipien:
  - Datenvermeidung und Datensparsamkeit [§ 3a BDSG]

„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.“

Bundesdatenschutzgesetz

- Grundprinzipien:
  - Verbot mit Erlaubnisvorbehalt
    *„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.“* [§ 4 (1) BDSG]
  - öffentliche und nicht-öffentliche Stellen müssen einen „Beauftragten für den Datenschutz“ bestellen [§ 4f BDSG]
    - Ansprechstelle bei Datenschutzproblemen
    - wichtig: Unabhängigkeit!
      - zur Zeit EU-Verfahren gegen Deutschland wegen mangelnder gesetzlicher Unabhängigkeit
    - Bundesdatenschutzbeauftragter (gewählt für 5 Jahre)

Bundesdatenschutzgesetz

- Grundprinzipien:
  - besonders geschützte Daten

    „Besondere Arten personenbezogener Daten sind Angaben über
    - die rassische und ethnische Herkunft,
    - politische Meinungen,
    - religiöse oder philosophische Überzeugungen,
    - Gewerkschaftszugehörigkeit,
    - Gesundheit oder
    - Sexualleben.“ [§ 3 (9) BDSG]

Bundesdatenschutzgesetz

- Grundprinzipien:
  - Auskunftsrecht, Recht auf Löschung und Berichtigung

    „Die Rechte des Betroffenen auf Auskunft (§ § 19, 34) und auf Berichtigung, Löschung oder Sperrung (§ § 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. “ [§ 6 (1) BDSG]

    „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.“ [§ 19 (1) BDSG]

Bundesdatenschutzgesetz

- Grundprinzipien:
  - Auskunftsrecht, Recht auf Löschung und Berichtigung

    „Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.“ [§ 20 (1) BDSG]

    „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.“

    [§ 20 (2) BDSG]

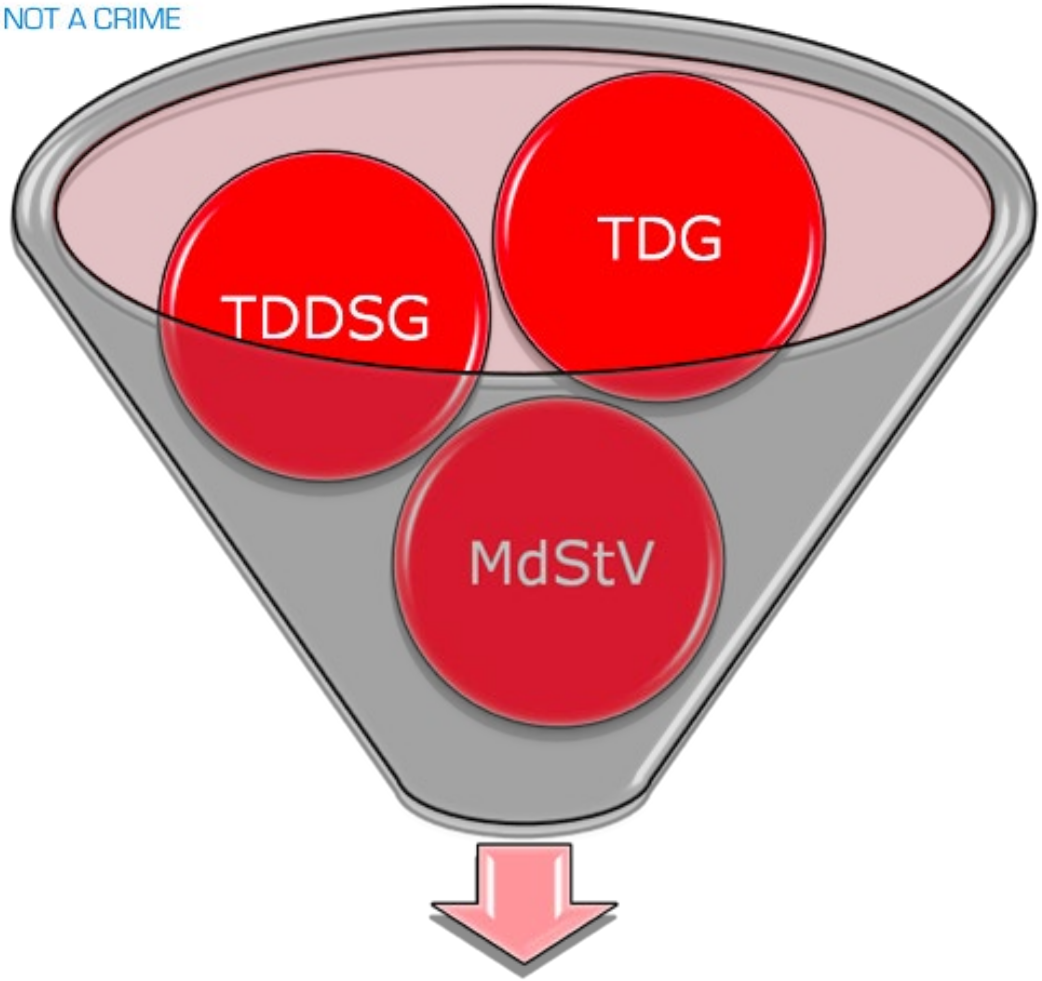
TK-Datenschutz: Um welche Art von Dienst handelt es sich? Historische Entwicklung

- Telekommunikationsdienste
  - Anknüpfungspunkt: Datentransport und Signalverarbeitung
  - Gesetzliche Regelung: TKG
  - Beispiele: Telefonkabel, Mobilfunk, Access-Provider, E-Mail
    - Speicherpflicht für Strafverfolgung

- Teledienste [bis 1. März 2007]
  - Anknüpfungspunkt: Inhalt der Kommunikation
  - Gesetzliche Regelung: TDG / TDDSG
  - Beispiele: Websites / Datendienste / Online Banking
    - Keine Verpflichtung zur Vorratsdatenspeicherung

- Mediendienste [bis 1. März 2007]
  - Anknüpfungspunkt: Inhalt mit redaktionellem Hintergrund
  - Gesetzliche Regelung: MDStV
  - Beispiele: Spiegel-Online, Heise etc.

Telemediengesetz



seit 1. März 2007: **Telemediengesetz** (TMG)

Telemediengesetz

- „Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179)“ (am 1.3.2007 in Kraft getreten)
- **§ 1 Anwendungsbereich**
  - (1) Dieses Gesetz **gilt für alle elektronischen Informations- und Kommunikationsdienste**, soweit sie nicht Telekommunikationsdienste ... sind (Telemedien).
  - (2) Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.
- **§ 4 Zulassungsfreiheit**
  - Telemedien sind im Rahmen der Gesetze **zulassungs- und anmeldefrei**.
- **§ 7 Allgemeine Grundsätze**
  - (2) Diensteanbieter im Sinne der §§ 8 bis 10 sind **nicht verpflichtet**, die von ihnen übermittelten oder gespeicherten Informationen **zu überwachen** oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.

§ 8 Durchleitung von Informationen

- (1) Diensteanbieter sind **für fremde Informationen**, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, **nicht verantwortlich**, sofern sie
  - 1. die Übermittlung nicht veranlasst,
  - 2. den Adressaten der übermittelten Informationen nicht ausgewählt und
  - 3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

§ 11 Anbieter-Nutzer-Verhältnis

- (2) Nutzer im Sinne dieses Abschnitts ist jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

§ 12 Grundsätze

- (1) Der Diensteanbieter **darf personenbezogene Daten** zur Bereitstellung von Telemedien **nur erheben** und verwenden, **soweit** dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es **erlaubt oder der Nutzer eingewilligt hat**.
- (2) Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene **personenbezogene Daten für andere Zwecke nur verwenden**, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es **erlaubt oder der Nutzer eingewilligt hat.**

§ 13 Pflichten des Diensteanbieters

- (4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass
  - 2. die anfallenden **personenbezogenen Daten** über den Ablauf des Zugriffs oder der sonstigen Nutzung **unmittelbar nach** deren **Beendigung gelöscht** ... werden,
  - 3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
  - 4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
  - 6. **Nutzungsprofile** nach § 15 Abs. 3 **nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können**.

- (6) Der Diensteanbieter hat die **Nutzung** von Telemedien und ihre **Bezahlung anonym oder unter Pseudonym zu ermöglichen**, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

- **§ 14 Bestandsdaten**
  - (1) Der Diensteanbieter darf **personenbezogene Daten** eines Nutzers **nur erheben** und verwenden, **soweit sie** für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien **erforderlich sind** (Bestandsdaten).
- **§ 15 Nutzungsdaten**
  - (1) Der Diensteanbieter darf **personenbezogene Daten** eines Nutzers **nur erheben** und verwenden, **soweit** dies **erforderlich** ist, **um** die **Inanspruchnahme von Telemedien zu ermöglichen** und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere
    - 1. Merkmale zur Identifikation des Nutzers,
    - 2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
    - 3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

Telemediengesetz

§ 16 Bußgeldvorschriften

- (2) **Ordnungswidrig** handelt, wer vorsätzlich oder fahrlässig
  - 4. einer Vorschrift des § 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5 über eine dort genannte **Pflicht zur Sicherstellung zuwiderhandelt**,
  - 5. entgegen § 14 Abs. 1 oder § 15 Abs. 1 Satz 1 oder Abs. 8 Satz 1 oder 2 **personenbezogene Daten erhebt** oder verwendet oder nicht oder **nicht rechtzeitig löscht** oder
  - 6. entgegen § 15 Abs. 3 Satz 3 ein **Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführt**.
- (3) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu **fünfzigtausend Euro** geahndet werden.

Vorratsdatenspeicherung in der EU

- geregelt in: „RICHTLINIE 2006/24/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG"
- Zweck: „Vorratsspeicherung bestimmter Daten … zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten"
- zu speichern sind: „Verkehrs- und Standortdaten … nicht … Inhalt elektronischer Nachrichtenübermittlungen"
- Speicherfrist: „mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation"
- Weitergabe der Daten: „nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden"

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Rückverfolgung und Identifizierung der Quelle einer Nachricht:
    - betreffend Telefonfestnetz und Mobilfunk:
      - die Rufnummer des anrufenden Anschlusses,
      - der Name und die Anschrift des Teilnehmers;
    - betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      - die zugewiesene(n) Benutzerkennung(en),
      - die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,
      - der Name und die Anschrift des Teilnehmers, dem eine Internetprotokoll-Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Identifizierung des Adressaten einer Nachricht benötigte Daten:
    - betreffend Telefonfestnetz und Mobilfunk:
      - die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,
      - die Namen und Anschriften der Teilnehmer;
    - betreffend Internet-E-Mail und Internet-Telefonie:
      - die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie,
      - die Namen und Anschriften der Teilnehmer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:
    - betreffend Telefonfestnetz und Mobilfunk:
      - Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs
    - betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      - Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers,
      - Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:
    - betreffend Telefonfestnetz und Mobilfunk:
      - der in Anspruch genommene Telefondienst
    - betreffend Internet-E-Mail und Internet-Telefonie:
      - der in Anspruch genommene Internetdienst

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:
    - betreffend Telefonfestnetz:
      - die Rufnummern des anrufenden und des angerufenen Anschlusses;
    - betreffend Mobilfunk:
      - die Rufnummern des anrufenden und des angerufenen Anschlusses,
      - die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,
      - die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,
      - die IMSI des angerufenen Anschlusses,
      - die IMEI des angerufenen Anschlusses,
      - im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:
    - betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
      - die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluß,
      - der digitale Teilnehmeranschluß (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:
  - zur Bestimmung des Standorts mobiler Geräte benötigte Daten:
    - die Standortkennung (Cell-ID) bei Beginn der Verbindung,
    - Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt

Vorratsdatenspeicherung in der EU

- Artikel 5 der EG-Richtlinie regelt detailiert, was für welche Art von Telekommunikationsdienst jeweils zu speichern ist:

  - „Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluß über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.“

Vorratsdatenspeicherung in der EU

⌘ Anforderungen an die Speicherung:

- Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung schützen
- Zugang zu den Daten ausschließlich besonders ermächtigten Personen ermöglichen
- Daten am Ende der Vorratsspeicherungsfrist vernichten, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind

- jedoch: Daten unverzüglich an die zuständigen Behörden auf deren Anfrage hin weiterleiten

- zusätzlich: Statistik über den Abruf von auf Vorrat gespeicherten Daten

Vorratsdatenspeicherung in der EU

Umsetzung und Evaluierung:

- Umsetzung in nationales Recht bis spätestens 15. September 2007
  - „Bis 15. März 2009 kann jeder Mitgliedstaat die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufschieben."
- Öffentliche Evaluierung „der Anwendung dieser Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher" spätestens am 15. September 2010
  - ggf. Anpassung der Liste von zu speichernden Daten (Artikel 5) sowie der Speicherfristen
- Hinweis: Irland hatte Klage gegen die Direktive vorm Europäischen Gerichtshof eingereicht
  - Grund: falsche Rechtsgrundlage für das Erlassen der Richtlinie
  - Klage wurde abgewiesen

Vorratsdatenspeicherung in Deutschland

- **„Gesetz zur Neuregelung der Telekommunikations-überwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG"** (21. 12. 2007)
  - Änderungen einer Vielzahl bestehender Gesetze

- Inkrafttreten: 1. 1. 2008 (für Internet-basierte Dienste: 1. 1. 2009)
  - Verfassungsbeschwerde von ca. 34 000 Klägern
  - Eilentscheidung:
    - Speicherverpflichtung bleibt grundsätzlich bestehen
    - Beschränkung der Verwendung
      - Katalogtat im Sinne von § 100a Strafprozeßordnung
  - endgültige Entscheidung:
    - 2. März 2010
      - aktuelle gesetzliche Regelungen hinfällig
      - Vorratsdatenspeicherung aber prinzipiell möglich

Änderungen im Telekommunikationsgesetz (TKG)

- neu: § 113a TKG „Speicherungspflichten für Daten“
  - Speicherfrist: 6 Monate
  - „(6) **Wer** Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift **zu speichernden Angaben verändert**, **ist zur Speicherung der ursprünglichen und der neuen Angabe** sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone **verpflichtet**.“
  - „(8) Der **Inhalt** der Kommunikation und **Daten über aufgerufene Internetseiten** dürfen auf Grund dieser Vorschrift **nicht gespeichert** werden.“

Gesetzesbegründung

- Hierbei kommt es auch nicht darauf an, ob die Zwischenschaltung des Diensteanbieters etwa aus technischen oder wirtschaftlichen Gründen durch die an der Erbringung der Telekommunikationsdienste beteiligten Diensteanbieter geschieht oder ob die Zwischenschaltung auf Veranlassung des Endnutzers gezielt zur Veränderung der nach Maßgabe der Absätze 2 bis 4 zu speichernden Daten erfolgt, wie dies etwa bei der Nutzung von **Anonymisierungsdiensten** der Fall ist. In beiden Fällen **besteht die Speicherungsverpflichtung nach Absatz 6**, wenn die maßgeblichen Daten bei der Erbringung des Telekommunikationsdienstes verändert werden.

- Auch **Anonymisierungsdienste weisen allerdings eine solche Doppelnatur auf**, da ihre Tätigkeit sowohl in der Durchleitung der Nachricht als auch in der Ersetzung der Ausgangskennung des Telekommunikationsnutzers besteht. Diese Dienste **sind daher sowohl Telemedien als auch** – im Hinblick auf ihre Transportfunktion – **Telekommunikationsdienste** für die Öffentlichkeit.

Strafprozeßordnung

- §§ 100 a, b und §§ 100 g relevant für Überwachungsmaßnahmen

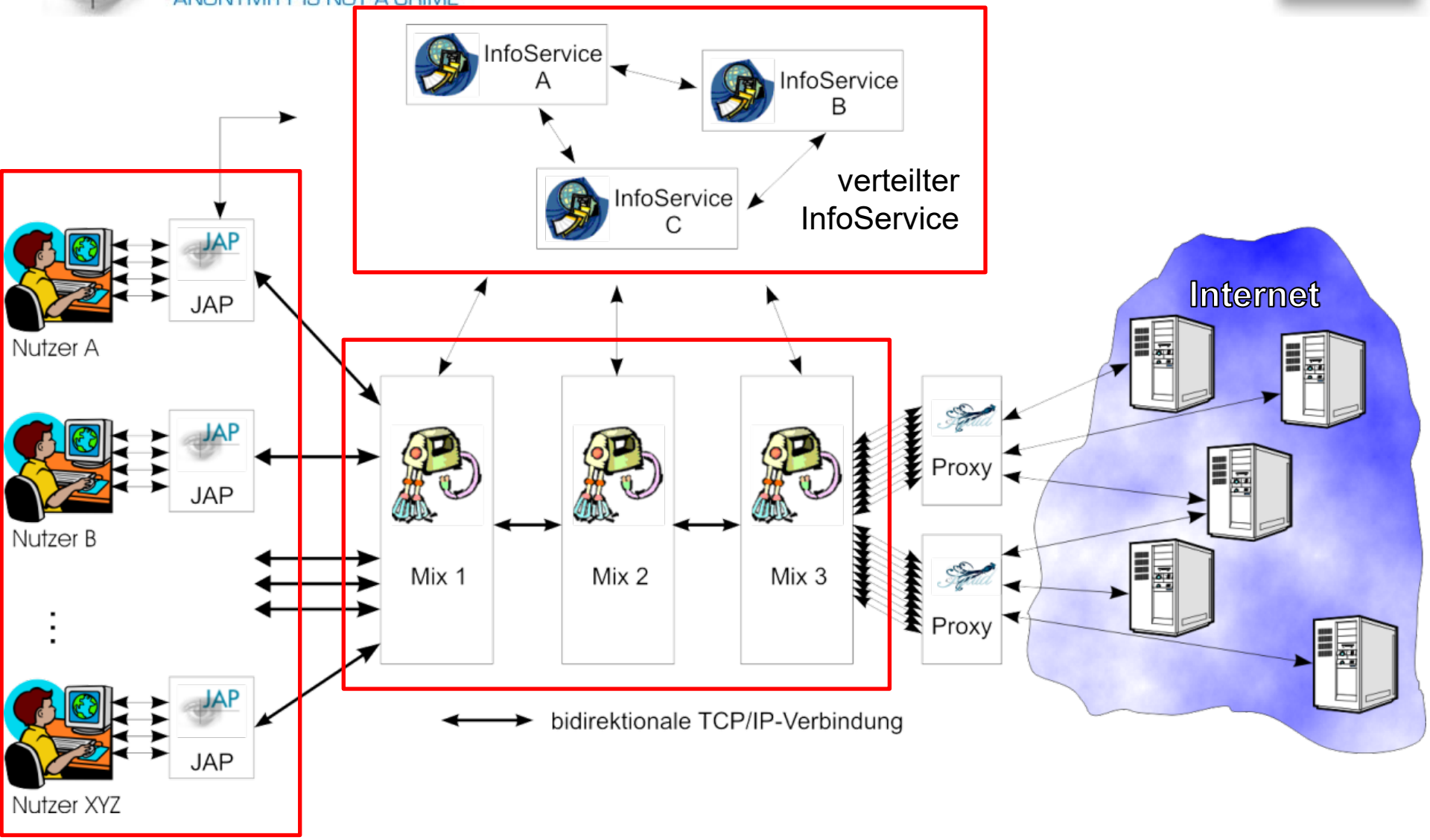
- §§ 100 g
  - **Auskunftsersuchen** ist auf Daten beschränkt, die nach bestehenden Regelungen zulässigerweise erhoben und gespeichert werden und insoweit bereits vorliegen

- §§ 100 a, b
  - **Aufzeichnung** personenbezogener Daten für die Zukunft kann angeordnet werden
  - Vorraussetzung:
    - Verdacht auf Straftat gemäß Katalog
    - richterliche Anordnung (maximal für drei Monate)
    - bei Gefahr im Verzug auch Staatsanwalt (maximal für drei Tage)

Aktuelle Entwicklungen

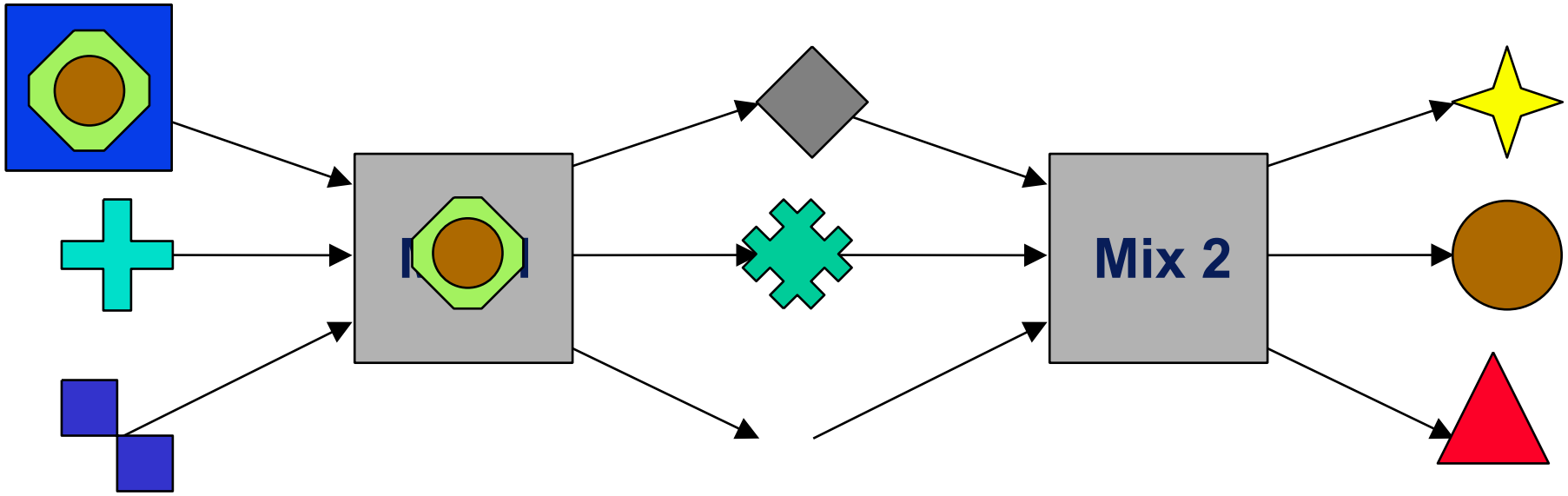
- EU-Datenschutzverordnung(!)
  - Entwurf vom 25. Januar 2012
    - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf
  - zur Zeit stark diskutiert
  - große Lobbying-Bemühungen der Wirtschaft sowie aus USA
    - Verschärfung der Datenschutzbestimmungen befürchtet
  - Vorteile aus wirtschaftlicher Sicht:
    - einheitliche europäische Regelungen
    - „One-Stop-Shop" für datenschutzrechtliche Belange
  - mögliche negative Auswirkungen aus deutscher Sicht:
    - Absinken des hohen deutschen Datenschutzniveaus

Überblick AN.ON-Gesamtsystem



Das Mix-Verfahren

Idee: Unverkettbarkeit zwischen ein- und ausgehenden Nachrichten erzeugen



Ein Mix sammelt Nachrichten, kodiert sie um und gibt sie umsortiert wieder aus.

Arbeiten ***alle*** Mixe zusammen,
können sie den Weg einer Nachricht zurückverfolgen.

Nutzung des Anonymisierungsdienstes

- kostenlos nutzbar seit September 2000
  - > 1 000 000 Downloads des JAP

- aktuelle Nutzung
  - geschätzt:
    - > 50 000 Nutzer
    - > 5 000 gleichzeitig
  - pro Monat:
    - > 18,75 TByte Daten
    - > 800 Million URLs

Mißbrauch von AN.ON

Jahr	gesamt	Anfragen von…	
		Strafverfolgungs-behörden	Privat-personen
2001	13	7	6
2002	40	15	25
2003	58	21	37
2004	61	38	23
2005	42	27	15
⋮	⋮	⋮	⋮

- aktuell monatlich:
  - ca. 2–4 Anfragen von Strafverfolgungsbehörden
  - ca. 3–6 Anfragen von Privatpersonen / Firmen

Mißbrauch verhinderbar?

- „künstliche" Beschränkung der unterstützten Protokolle
  - keine TCP/IP-Verbindungen möglich
    - implementiert aber deaktiviert
  - nur HTTP (Web)
  - nur bekannte HTTP-Ports (80, 443, 8080)
  - Begrenzung der Größe von POST-Anfragen (Uploads)
- Betreiber von Web-Seiten können Sperrung beantragen

- Mißbrauch aber generell nicht verhinderbar:
  - Zugriffe, die in einem Land zulässig sind, können in einem anderen Land verboten sein.
  - Rechner sind generell nicht in der Lage zu entscheiden, ob ein Zugriff „gut" oder „böse" ist.

Beispiel für Anfrage bei Mißbrauch

Polizeidirektion XY
Kommissariat 3

Berlin, den 25.02.2005

Ermittlungsverfahren gegen Unbekannt wegen des Verdachtes auf Computerbetrug

Sehr geehrte Damen und Herren,
im Rahmen des oben genannten Ermittlungsverfahrens wurde festgestellt, daß dem Täter eine IP-Adresse zugeordnet werden kann, die durch Sie verwaltet wird:

IP-Adresse: **141.76.1.121**
Datum/Uhrzeit: **25.06.2004, 09:05:46 Uhr**

Sie werden nun gebeten, alle Ihnen bekannten Verbindungs- und Nutzungsdaten mitzuteilen, die oben genannte IP-Adresse und Zeitpunkt betreffen. Es wird auch um Mitteilung gebeten, falls keine Daten zum Beispiel auf Grund der bereits verstrichenen Zeit vorliegen.

Beispiel für Antwort bei Mißbrauch

Lehrstuhl Datenschutz & Datensicherheit Dresden, den 26.02.2005
TU Dresden

Ermittlungsverfahren gegen Unbekannt wegen des Verdachtes auf Computerbetrug

Sehr geehrte Damen und Herren,

... Der von Ihnen genannten Server ist Teil eines Forschungsprojektes. Ziel des Projektes ist es, anonyme und unbeobachtbare Webzugriffe zu realisieren. Dabei geht es darum, die Vorschriften des Teledienstedatenschutzgesetzes umzusetzen.
Dabei wird bereits auf technischer Ebene die Zuordnung von IP-Adressen zu einzelnen Nutzern oder sonstigen identifizierenden Merkmalen vermieden. Aus diesem Grunde liegen keine Daten vor, über die (bei Vorliegen eines richterlichen Beschlusses) Auskunft gegeben werden könnte.
Es tut mir leid, Ihnen insoweit nicht weiterhelfen zu können. ...

Der BKA Fall

- 03.07.2003: Beschluß des Amtsgerichts Frankfurt/Main
  - Grundlage: §§ 100g, 100h StPO
  - Speicherung / Auskunft von Zugriffen auf eine bestimmte IP
  - ULD legt Beschwerde ein (keine aufschiebende Wirkung)
- Einbau / Aktivierung der Strafverfolgungsfunktion
  - Aufzeichnung eines einzelnen Datensatzes
- 11.07.2003: Landgericht Frankfurt setzt Vollziehung aus
  - Mitteilung an ULD erst 26.08.2003
  - Bestätigung endgültig 15.09.2003
- 29.08.2003: AG Frankfurt ordnet Durchsuchung der Räume der TU Dresden und Beschlagnahme an
  - Auskunftsverpflichtung war schon ausgesetzt
  - Protokolldatensatz wird unter Protest herausgegeben
- 21.10.2003: LG Frankfurt bestätigt Rechtsauffassung des ULD
  - Durchsuchungsanordnung und Beschlagnahme waren rechtswidrig
- Löschung des Datensatzes erweist sich als schwierig

Stoffsammlung Kultur

- http://www.heise.de/newsticker/meldung/Britischer-Medienoekonom-schlaegt-Boersenplatz-fuer-Rechtehandel-vor-1245905.html
- http://www.heise.de/newsticker/meldung/USA-Amazon-verkauft-mehr-digitale-als-gedruckte-Buecher-1246227.html
- http://www.heise.de/newsticker/meldung/Googles-Think-Tank-stoesst-Debatte-um-neues-Urheberrecht-an-1209532.html
- http://www.heise.de/newsticker/meldung/Copyright-Forscher-Das-Urheberrecht-passt-nicht-mehr-1135978.html

Merker

- BSI Grundschutzmodul Datenschutz

Gewissensbits: Diskussion hypothetischer – aber relevanter – Anwendungsfälle

- Fallbeispiele basierend auf dem Buch:

  Debora Weber-Wulff, Christina Class, Wolfgang Coy, Constanze Kurz, David Zellhöfer: „Gewissensbisse – Ethische Probleme der Informatik – Biometrie – Datenschutz – geistiges Eigentum“, transcript Verlag, Bielefeld, 2009

- weitere Fallbeispiele von Zeit zu Zeit in der Zeitschrift „Informatik Spektrum“, Organ der GI

- https://gewissensbits.gi.de/

Fallbeispiel 1: Biometrie

- Andy, Informatiker an Schule
- Aufgabe: neues Bezahlsystem für Mensa
  - Bezahlung basierend auf Fingerabdruck
  - Fingerabdrücke sicher in Schul-Datenbank gespeichert
  - ➔ falls nicht gewünscht / nicht möglich: Barzahlung (3% Aufschlag)

- dann: Beamer-Diebstahl
  - Anweisung vom Direktor: Fingerabdrücke an Polizei

Fallbeispiel 1: Biometrie – Fragen

- Werden Kinder, die keine qualitativ ausreichenden Fingerabdrücke in der Schuldatenbank hinterlegen können, diskriminiert?
- Ist es ethisch vertretbar, dass wer aus persönlicher Ablehnung das Bezahlsystem nicht benutzen möchten, dazu gezwungen wird, den Aufschlag zu zahlen?
- Ist es hinnehmbar, dass die Privatsphäre der Kinder verletzt wird?
- Ist es eine ethisch vertretbare Herangehensweise des Direktors, den Kindern den Diebstahl zu unterstellen?
- Muß Andy die Polizei auf die Datenbank aufmerksam machen?
- Wie schwerwiegend ist der Vertrauensbruch, der mit der freiwilligen Weitergabe der biometrischen Daten verbunden ist?
- Welchen Entscheidungsspielraum hat Andy tatsächlich?
- Sollen vor der Herausgabe zumindest die Eltern und Kinder unterrichtet werden?

Fallbeispiel 2: „Zivilitäre“ Forschung

- Tobias, Informatiker an Uni in Robotik-Projekt
  - schon als Student im Projekt
- Juliane, Leiterin
- Zusammenarbeit mit externer Forschungsgruppe
  - zunächst unbekanntes Ziel der externen Forscher: „Soldaten der Zukunft“
- Beschwichtigung von Julian:
  - Forschung immer mit Potential für „dual use“
  - Militärische Forschungsergebnisse auch nützlich im zivilen Umfeld

Fallbeispiel 2: „Zivilitäre“ Forschung – Fragen

- Ist es ein ethisches Problem, dass sich Tobias einfach keine Gedanken dazu gemacht hat?
- Hätte er sich mit den Fragen nach dem sogenannten „Dual Use“, der zivilen und militärischen Nutzung derselben Technologie, von sich aus beschäftigen müssen?
- Kann er überhaupt an autonomen Robotern arbeiten, ohne mittelbar militärische Forschung zu unterstützen?
- Wäre es gar kein Problem, wenn er Militärforschung für ein notwendiges Forschungsgebiet hielte?
- Darf er seine pazifistische Haltung einfach in ein Forschungsprojekt einbringen?
- War Juliane verpflichtet, die Programmierer über den Zweck des neuen Kooperationsprojektes zu unterrichten?
- Hat sie gegenüber ihrem Untergebenen Tobias angemessen argumentiert, als sie ihm sagte, sie hätte keine Unruhe stiften wollen?
- Wie sollte sich Juliane als Projektleiterin prinzipiell zu dem Problem „Dual Use“ stellen?
- Muss sie es thematisieren, auch wenn sie selbst kein Problem darin sieht?
- Darf jemand die Arbeit an so einer Technologie aus Gewissensgründen verweigern?
- Was hilft es, wenn sich Tobias gegen eine Mitarbeit an potentieller Rüstungstechnologie entscheidet, wenn er genau weiß, dass andere seine Arbeit ohnehin fortführen?

Fallbeispiel 3: Finanzportal

- Nora, Systemanalytikerin, Investment-Portal
  - 2 Kinder, Haus
- Felix, Chef
  - Anforderung: Empfehlungssystem für Finanzinvestitionen
- Ralf, Projektleiter Implementierung
  - Frage: Woher Präferenzliste für Empfehlungssystem
- Antwort Felix: Gemäß Bezahlung durch Kunden

Fallbeispiel 3: Finanzportal – Fragen

- Besteht hier ein ethisches Problem? Wie kann das Handeln der drei Personen Felix, Nora und Ralf beurteilt werden? Sind Aspekte der Ethischen Leitlinien der GI angesprochen?
- Welche Handlungsalternativen gibt es für Nora? Und für Ralf? Oder für Felix? Wäre es anders, wenn der vorgeschlagene Fonds tatsächlich auf der Basis eines umfangreichen Analyse-Algorithmus ermittelt würde?
- Ist es ein Betrug am Kunden? Wenn ja, wer trägt die Hauptschuld an diesem Betrug an den Kunden? Kann man überhaupt jemandem eine Schuld zuweisen? Wird Nora als weisungsgebundene Angestellte überhaupt mitschuldig? Wenn ja, wie unterscheidet sich ihre Verantwortung von der von Ralf und Felix? Gibt es eine strafrechtliche Seite (StGB § 263 Betrug , § 264 Computerbetrug)? Trägt Nora Mitverantwortung?
- Was änderte sich, wenn Nora in einer weniger schwierigen persönlichen Lage wäre? Wäre sie finanziell unabhängig, müsste man dann höhere ethische Standards anlegen? Darf ihre persönliche Situation überhaupt Einfluss auf ihre Entscheidung haben?

Strafgesetzbuch (StGB) § 263 Betrug

- (1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- (2) Der Versuch ist strafbar.

Strafgesetzbuch (StGB) § 264 Computerbetrug

- (1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- (3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Fallbeispiel 3: Finanzportal – Fragen

- Wenn Nora in ihrer finanziellen Situation keine andere Chance sieht, sollte sie ihr Wissen vielleicht anonym veröffentlichen? Ist es für Nora vertretbar, zwar das gewünschte Programm zu schreiben, ihr Gewissen aber nachher dadurch zu entlasten, dass sie den Betrug z. B. in einem Internet-Forum für Aktienanlagen offenlegt?
- Sie fragt sich, ob es nicht besser sei, das Geld ihres betrügerischen Chefs zwar zu nehmen, ihn dann aber zu enttarnen. Sie muss in diesem Fall jedoch fürchten, als Quelle der Information enttarnt zu werden. Kann sie sich davor schützen?
- Wenn sich die Betrügerei nach einer Veröffentlichung im Forum herumspricht, wird dies nicht auch Folgen für Noras Arbeit haben können? Die Firma SicherInvest können Kunden verlieren oder sogar pleitegehen, damit wäre auch Noras Job gefährdet.
- Ist es überhaupt von Bedeutung, wenn Nora sich weigert, bei
- der Erstellung des Programms mitzuarbeiten? Sie weiß ja, dass dieser Programmteil leicht geschrieben werden kann. Andere Programmierer für das Projekt wären leicht gefunden. Spielt es ethisch eine Rolle, dass Nora leicht ersetzbar ist?