
BIG DATA zwischen Heilserwartung, Horror und Mythos

Dr. Thilo Weichert, Leiter des ULD

IUK-Branchenforum
„Big Data – wer weiß mehr?“
Hannover, 19. Februar 2015

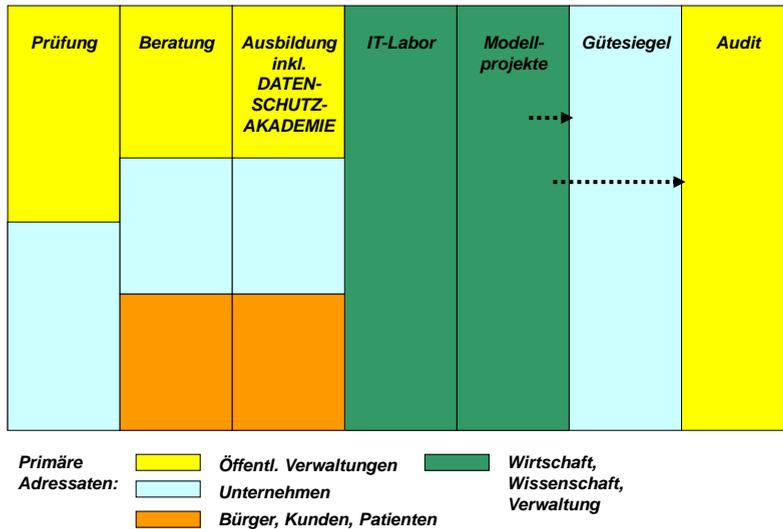


www.datenschutzzentrum.de

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Vertraulichkeit und Recht
- Datenquellen, Zielsetzungen, Anwendungen
- Risiken
- Schutzziele des Datenschutzes
- Datenschutzmechanismen
 - Anonymisierung
 - Transparenz
 - Regulierung
- Schlussfolgerungen

Datenschutz und Informationsfreiheit



Big Data

3+1 Vs von Big Data

- Volume
- Variety
- Velocity
- > Value

Versprechen

- Kostenersparnis und Profit
- Wissenschaftlich fundierte Erkenntnis > Prognosen
- Personalisierte Entscheidungen
- Effiziente gesellschaftliche Planung und Organisation
- > Goldgrube für IT-Wirtschaft

Vertraulichkeit und Recht

- Berufliche Vertraulichkeitsversprechungen
- Datenschutzrecht seit den 70er Jahren > BDSG, LDSGs, Europäische Datenschutz-Richtlinie 1995
- 1983: Volkszählungsurteil des BVerfG > Grundrecht auf informationelle Selbstbestimmung
- 2008: Onlinedurchsuchungsurteil des BVerfG > Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme
- 2009: Art. 8 Europäische Grundrechtecharta mit DS
- Spezialnormen: TKG, TMG, SGB und viele, viele mehr

Grundrechte

Pro Sammlung und Analyse:

Berufsfreiheit, Eigentum, Forschungsfreiheit, Informations- und Meinungsfreiheit

Contra Sammlung und Analyse:

Allgemeines Persönlichkeitsrecht (informationelle Selbstbestimmung, digitale Privatsphäre, Telekommunikationsgeheimnis, digitale Freiheiten (vgl. politische analoge Freiheitsrechte), Diskriminierungsverbot, Verbraucherschutz, Anspruch auf Rechtsschutz

Generelle Gültigkeit

> Drittwirkung, staatliche Schutzpflichten

USA

- Keine digitalen Grundrechte (schon gar nicht für Ausländer)
- US-Supreme Court: Reasonable Expectations of Privacy
- Vorrang der Sicherheitsbelange
- Keine (gesetzliche) Bindung von Privaten
- Third Party Doctrine

1890 - Warren/Brandeis: „Right to Privacy“

1967 - Westin: „Privacy and Freedom“

Seitdem keine rechtsstaatliche Weiterentwicklung trotz verfassungsrechtlicher Grundlagen in Amendments

- > Sicherung der globalen Sicherheitshegemonie
- > Sicherung der globalen wirtschaftlichen Hegemonie

Big-Data-Anwendungen

- Internet (Info+Komm, Soziale Netzwerke, Suchen, Apps)
- Werbewirtschaft, Handel (CRM)
- Finanzdienstleister (Kredit, Versicherung: Scoring, Rating)
- Branchenwarnsysteme (z. B. Wohnung, Reise)
- Medizin, Gesundheitswesen
- Mobilität, Verkehr
- Arbeitsverhältnis
- Organisation und Planung
- Forschung, Wissenschaft
- Selbstoptimierung,

Öffentlicher Bereich: Geheimdienste, Polizei (z. B. predictive policing), Gesetzliche Krankenversicherung

Beispiel Geheimdienste

Seit Juni 2013: Enthüllungen durch Edward Snowden
Politische und wirtschaftl. Spionage, Vollüberwachung der
Bevölkerung zw. Terrorismusbekämpfung

- National Security Agency (NSA - USA): Prism u. a.
- Government Communications Headquarters (GCHQ – GB):
Tempora u. a.
- Direction Générale de la Sécurité Extérieure (DGSE – F)
- Bundesnachrichtendienst (BND – D): Strateg. TKÜ u. a.
- Weitere Five Eyes (Kanada, Australien, Neuseeland)
- Spionage aus China, Russland...

Datenquellen

- Abgreifen von Internetdienstleistern, z. B. Soziale Netzwerke od.
Clouds (in den USA, zwangsweise od. freiwillig)
- Verdeckter Zugang zu einem Netzbetreiber (GCHQ-BelgaCom)
- Brechen von Kryptografie
- Verdeckter Zugang zu Internetdiensten (über Backdoors) zur
Beschaffung von Meta- und Inhaltsdaten (z. B. Adressbücher)
- Abhören von Internetkabeln oder von Internetknoten
- Beschaffung von (evtl. zulässig erlangten Daten von) „befreundeten“
Diensten (z. B. strategische BND-TKÜ)
- Kapern von Rechnern und Rechnernetzen (unterschiedliche Methoden,
z. B. Online-Durchsuchung)
- Verdeckte technische und personale Ermittlungen
- Sammeln und Auswerten „öffentlicher Quellen“ (z. B. im Netz)

Risiken

Für Betroffene

- Beeinträchtigung der Vertraulichkeit (z. B. bei Inanspruchnahme von Hilfe)
- Beeinträchtigung der Wahlfreiheit
- Diskriminierung (z. B. Bonus-Malus-Systeme)
- Manipulation
- Körperliche und seelische Schäden
- Kommerzielle Ausbeutung

Für anwendende Stellen

- Ansehensverlust, Akzeptanzverlust für bes. Maßnahmen
- Finanzielle Schäden

Für Demokratie, Freiheitsrechte, Rechtsstaatlichkeit algorithmusgesteuerte Gesellschaft?

Schutzziele des Datenschutzes

- **Vertraulichkeit** (z.B. Verschlüsselung)
- **Integrität**, Authentizität (Backup, digitale Signatur)
- **Verfügbarkeit** (ausfallsichere Stromversorgung, Datenmanagement)
- **Intervenierbarkeit** (Löschen, Sperren, Beauskunften)
- **Unverknüpfbarkeit** (Abschottung, Datensparsamkeit)
- **Transparenz**, Revisionsfähigkeit (Protokollierung, Kontrolle der SysAdmin, Dokumentation, Anwenderhandbücher, Information bei Erhebung, Benachrichtigung bei Bearbeitung)

Schutzziele und Big Data

- Vertraulichkeit: nur nach Anonymisierung
- Integrität: bei vielen Datenquellen – z. B. Internet – unklar
- Verfügbarkeit: relevant bei Echtzeit-Analysen
- Intervenierbarkeit: Betroffenenrechte bisher kein Thema
- Transparenz: Betriebs- und Geschäftsgeheimnisse
- Nichtverkettbarkeit: No go

7 Regeln des Datenschutzes

- Rechtmäßigkeit (Verbot mit Erlaubnisvorbehalt)
- Einwilligung (bestimmt, freiwillig, widerrufbar)
- Zweckbindung (bei jedem Verarbeitungsschritt)
- Erforderlichkeit und Datensparsamkeit
- Transparenz und Betroffenenrechte
- Datensicherheit
- Kontrolle

Rechtmäßigkeitsvoraussetzungen

- Gesetzliche Regelungen
- Festlegungen von Daten Zweck und Stellen
- Ebenso bei Einwilligungen
- Interessenabwägung bei jeder Form der Datenverarbeitung
- Information, Erklärung
- technisch-organisatorische Vorkehrungen
- Verfahrenssicherungen (Genehmigungen u. Ä.)
- Anonymisierung/Aggregation

Anonymisierung

- Ersetzen der Identifikatoren (Betroffener, Erhebungsstelle, Dienstleister)
- Aggregation (Datensätze, Merkmale) – abhängig von Quantität, Qualität und Gewichtigkeit der Datensätze
 - > Anonymität führt zu Qualitätsverlust

Lösungen:

- Register mit Treuhänder
- Forschungsgeheimnis u. qualifizierte Einwilligung
- Datentransparenz unter staatlicher Aufsicht und Kontrolle (§§ 303a SGB V)
- Mehrschichtige Pseudonymisierungsverfahren (Problem: unendliches Zusatzwissen)

Transparenz

Adressaten (mit differenziertem Informationszugang):

- Betroffener (evtl. gar ein „Recht auf Nichtwissen“),
- Erhebende Stelle, Dienstleister, Bedarfsträger
- (staatliche) Aufsicht, Verwaltungs-Hierarchie
- Demokratisch legitimierte und rechtliche Genehmigungs- und Kontrollinstanzen (z. B. DS-Aufsicht, Fach- und Wirtschafts-Aufsicht, Parlamente, Gerichte)
- (wissenschaftliche) Fachöffentlichkeit
- Öffentlichkeit

Inhalte: Input, Output, Verfahren, Prozesse, Algorithmus, Sicherungen, Kontrolle, aber Betriebs- und Geschäftsgeheimnisse

Regelungsbedarf

- Regelungswirrwarr (Bund/Land – Europa/Staat – Wirtschaft/Verwaltung – Zwecke/Adressat)
- Informations- und Schutzbedarfe abdecken
- Bestehende Ansatzpunkte: Registergesetze, Transparenz- und Informationszugangsregelungen, Netz-Regulierung,
- Selbstregulierung (Kammern, Branchen, Forschungsgemeinschaften) Best Practice, SOPs, Verhaltensregeln
- Europäische Datenschutzgrundverordnung (Art. 20 E)

Die großen Irrtümer

- Daten sind nicht Informationen
- Informatik ist nicht Semantik
- Korrelation ist nicht Kausalität
- Digitale Analytik ist nicht Wahrheit
- Werte und Gefühle sind nicht digitalisierbar

Schlussfolgerungen

- Stärkung des Wissens- und IT-Standorts
- Verbesserung der gesellschaftlichen (politischen, wirtschaftlich, Infrastruktur) Angebote
- Stärkung der individuellen Selbstbestimmung
- Staatliche Angebote (Private-Public-Partnership, TransparenzR, IT-Strukturen)

BIG DATA zwischen Heilserwartung, Horror und Mythos

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-
Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

<https://www.datenschutzzentrum.de>