# Datenschutzgerechte Sicherheitstechnik

Thilo Weichert, Leiter des ULD

VfS-Kongress 2010: Mit der Sicherheitsbranche im konstruktiven Dialog

Leipzig 20.04.2010

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Beispiel INDECT
- Grundrechtsschutz und Sicherheit
- Grundrechtsfreundliche Sicherheitskultur
- Sicherheitstechnikanwendungen und Grundrechtsrisiken
- Aspekte datenschutzfreundlicher Sicherheitstechnik
- Internationale Dimension
- Schlussfolgerungen

# Unabhängiges Landeszentrum für Datenschutz

- Datenschutzkontrollinstanz im öffentlichen wie im nicht-öffentlichen Bereich (u.a. Polizei, Justiz, Geheimdienste, Detekteien, Sicherheitsunternehmen, Eigenschutz)
- Ausbildung, Beratung und Unterstützung von Betroffenen, Politik, Verbänden, verarbeitenden Stellen
- Erstellung von Gutachten und Stellungnahmen, auch für Gerichte (z.B. Kfz-Kennzeichen-Scan, Körperscanner)
- Durchführung von Projekten (u.a. Privacy and Security – PRISE, 2006-2008)
- Datenschutz-Gütesiegel und –Audit (seit 2001, incl. European Privacy Seal – EuroPriSe, seit 2008)





# Beispiel INDECT

- INDECT = Intelligentes Informationssystem zur Unterstützung von Beobachtung, Suche und Erkennung für Bürgersicherheit in städtischer Umgebung
- 2009-2013, Kosten 15 Mio. Euro, 17 Partner, 11 Staaten
- Ziel: Erkennen verdächtigen Verhaltens>Datensammeln> Auswertung>Einschaltung Sicherheitsbehörden

➢ Unwirtschaftliche Verausgabung öffentlicher Gelder
➢ Grundrechtsgefährdung durch Einsatz v. Sicherheitstechnik
➢ Beeinträchtigung von Compliance und Akzeptanz
➢ Verbreitung von grundrechtsgefährdender Technik, evtl. auch in Diktaturen

# Einführende Thesen

- Sicherheitstechnik ist heute auf Datenmaximierung und maximale Datenauswertung ausgerichtet
- Sicherheitstechnik hat Demokratie und Freiheitsrechte bisher noch nicht entdeckt
- Sicherheitstechnik scheut die Öffentlichkeit und die demokratische Kontrolle
- Die Menschen haben Angst vor Sicherheitstechnik
- Sicherheitstechnik gefährdet oft die Sicherheit





# Grundlagen des Datenschutzes

- Menschenwürde und allgem. Handlungsfreiheit (Art. 2 I i.V.m. 1 I GG), allgem. Pers.R. > Grundrecht auf Datenschutz (informationelle Selbstbestimmung, Privatheit)
- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG U.v. 27.02.2008 – Online-Durchs.; sog. „Computergrundrecht“)
- Recht auf Datensicherheit (BVerfG U.v. 02.03.2010 – Vorratsdatenspeicherung)
- Digitaler Grundrechtsschutz (Telekommunikation, Beruf, Eigentum, Wohnung, Familie, Religion, Asyl usw.; Information, Meinung, Presse)
- Europ. u. globaler digitaler Grundrechtsschutz (z.B. GR-Charta)

# Aspekte digitalen Grundrechtsschutzes

- Information (Wissen und Wissenkönnen)
- Wahlfreiheit (Bestimmen und Bestimmenkönnen)
- Gesellschaftliche Transparenz
- Eingriffe, verhältnismäßig, auf gesetzlicher, bestimmter verhältnismäßiger Grundlage
- Technisch-organisatorische Schutzvorkehrungen (Verschlüsselung, sicherer Zugriff, getrennte Speicherung, Protokollierung, Mehraugenprinzip)
- Prozedurale Schutzvorkehrungen (Entscheidungsvorbehalt, z.B. d. Richter, Beteiligungspflichten, Benachrichtigungs-pflichten, Beschwerdestellen, Rechtsschutz)





# Materielle Grundrechtsgewährleistungen

- Verbot umfassender Persönlichkeitsprofile
- Verbot von Personenkennzeichen
- Verbot der Rundumüberwachung
- Verbot der Vorratsdatenverarbeitung (anlasslose Kontrolle, „ins Blaue hinein“)
- Ausnahmecharakter der verdeckten Erhebung
- Schutz des Kernbereichs persönlicher Lebensgestaltung
- Individueller Systemschutz (Integrität, Vertraulichkeit eigengenutzter IT-Systeme)
- Struktureller Systemschutz (Verbot der Totalerfassung als „verfassungsrechtliche Identität der BRD“, Strafverfolgung, Gefahrenabwehr, IT-Infrastruktur)

# Grundlagen der Sicherheit

- Annäherungen: Gewaltabwehr, Rechtssicherheit, soziale Sicherheit, nicht nur Terrorismusbekämpfung
- Fließender Übergang innere-äußere Sicherheit (klassischer Grundrechtsschutz nur bei innerer Sicherheit)
- Fließende Übergänge Persönlichkeitsschutz und Geheimschutz aus sonstigen Gründen (Datenschutzverstöße als Sicherheitsgefahr)
- Digitale Risiken als Ergänzung und Eskalation analoger Gefahren mit dem Bedarf nach digitaler Reaktion





# Ziele grundrechtsorientierter Sicherheit

- Keine Angst vor Freiheitswahrnehmung
- Freiheit vor Manipulation
- Verhinderung von Diskriminierung
- Gesellschaftliche Solidarität, Verhinderung sozialer Spaltung
- Vermeidung von Aggressionsquellen
- Förderung grundrechtsfreundlicher Kultur, Bekämpfung grundrechtsfeindlicher Bestrebungen (In- u. Ausland)

➢ Sicherheitstechnik muss rechtmäßig sein (Compliance)

➢ Sicherheitstechnik muss ethisch vertretbar sein (Ethik als Lückenbüßer zum Recht und Langfristorientierung)

# Anwendungsbereiche der Sicherheitstechnik

- Kommunikationstechnik
- Biometrie
- Erfassungstechniken
- Datenspeicherung
- Auswertung und Entscheidungshilfe





# Kommunikationstechnik

- Festnetztelefonie
- Mobiltelefonie
- Internet (IP, Telemediendienste, Cloud-Anwendungen)
- Lokalisierungs- und Ortungssysteme (z.B. GPS, GSM)

➢ Abhören und strukturelle Überwachung von Kommunikation, Eingriffe in Privatsphäre, Freiheitssphären, individuelle räumliche und zeitliche Zuordnungen

# Biometrie

- Körperliche Merkmale (z.B. Gesicht, Fingerabdruck, Iris, Stimme, Schriftzug)
- DNA-Profil (genetischer Fingerabdruck)

➢ Authentifizierung, Autorisierung, Identifizierung
➢ Gefahr des Identitätsdiebstahls
➢ Verhinderung von Diskriminierung (false positives, false negatives)





# Erfassungstechniken

- Elektro-optische Sensoren (z.B. Videoüberwachung, CCTV, Infrarot)
- Durchstrahlungstechnologien (z.B. Terahertz-, Röntgen)
- Luft- und Satellitenüberwachung (z.B. Drohnen)
- Akustische Sensoren
- Physikalische/chemische Sensoren (z.B. Sprengstoffschleusen, Metalldetektoren)
- RFID
- Maschinenlesbare Dokumente (z.B. Reisepass, Ausweise u. ID-Karten, Kfz-Kennzeichen)
- Mustererkennung

➢ Eindringen in Intim- und Schambereich
➢ Gefahr der Falschverdächtigung
➢ Gefahr der Langfristspeicherung und der Verkettung

# Datenspeicherung

- Bevölkerungsdatenbestände (z.B. Melderegister, Zentrale Steuerdatei)
- Sicherheitsdateien (INPOL, NADIS, Schengen, Europol)
- Gruppendatenbestände (z.B. Eurodac)
- Privat-öffentliche Datenspeicherung (Kontodaten, TK-Daten, ehem. TK-Vorratsdaten, PNR, SWIFT)
- Private Datenbanken (CRM, Telemedien
- Datenbestände beim Betroffenen (PC, Mobilgerät)
- Bio(forschungs)banken

➢ Gefahr der Verknüpfung und Zweckentfremdung

➢ Gefahr der Dauerspeicherung und der Veröffentlichung





# Auswertung und Entscheidungshilfe

- Suchmaschinen
- Data Mining
- Mustererkennung
- Scoring (Wahrscheinlichkeitsprognosen)
- Automatische Entscheidungssysteme

➢ Gefahrenabwehr, Strafverfolgung

➢ Eingriff in persönliche Freiheitswahrnehmung

➢ Manipulation

➢ Diskriminierung

# Aspekte datenschutzfreundlicher (Sicherheits-)Technik

- Datensparsamkeit/Datenvermeidung (Anonymität, Pseudonymität, contra Massenverarbeitung, contra hohe Eingriffstiefen)
- Strenge Erforderlichkeitsprüfung
- Zugriffs- und Nutzungskontrollen
- Unverknüpfbarkeit (Pseudonymität, Verschlüsselung)
- Individuelle und gesellschaftliche Transparenz
- Anwendungsfreundlichkeit (Mensch-Maschine-Schnittstelle)
- Fehlerfreundlichkeit





# Lebenszyklus einer (Sicherheits-)Technik

- Prozessgestaltung > Datenschutzmanagement
- Forschung/Entwicklung > Standardisierung
- Zertifizierung > unabhängige und transparente Einzelprüfung
- Vermarktung > Ausschreibungskriterien
- Implementierung > Vorabkontrolle (Dokumentation, Test, Freigabe)
- Betrieb > Evaluierung, Sunshine-Klauseln, Audit, DMS

# Internationale Dimension

- Internationale Menschenrechtscharta (digital?)
- Europäische Grundrechtecharta/EU-Datenschutz-Richtlinien
- Datenschutz als globaler IT-Wettbewerbsfaktor (Hindernis, Marktvorteil)
- Globale Bekämpfung des Cyber Crime
- Export von Überwachungstechnologie in Unterdrückungsgesellschaften





# Schlussfolgerungen

- Schwarz-Weiß-Denken muss aufgegeben werden
- Kästchendenken muss aufgegeben werden
- Globale Datenschutzregulierung ist nötig
- Datenschutz muss Marktrelevanz erhalten
- Sicherheitstechnik muss sich der Gesellschaft öffnen

# Datenschutzgerechte Sicherheitstechnik

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de