Mit Recht und Gesetz gegen ausufernde digitale Kriminaltechnik?

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein

Tagung des Republikanischen Anwältinnen- und Anwältevereins e.V. (RAV)
„Neue digitale Schnüffelwerkzeuge"
Berlin, 04.02.2012

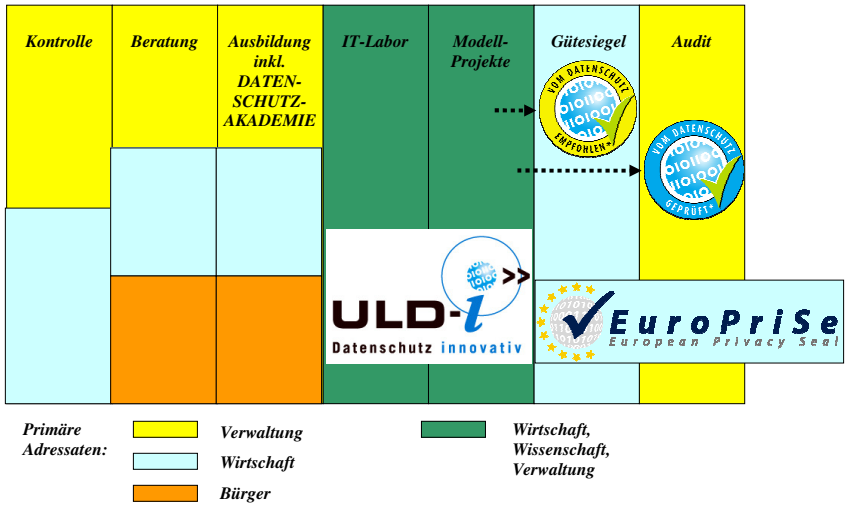
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Entwicklung, Stand und Tendenzen bei der digitalen Kriminaltechnik
- Parlamente
- Presse, Wissenschaft und Non-Governmental Organzations
- Betroffenenrechte
- Datenschutz
- Gerichte
- Perspektiven

ULD www.datenschutzzentrum.de

Unabhängiges Landeszentrum für Datenschutz



ULD www.datenschutzzentrum.de

Entwicklung polizeiliche Datenverarbeitung

- Seit Bestehen der Kriminalpolizei: Diebeslisten und Register
- Kriminalakten und Aktennachweise, 50er Lochkarten
- 13.11.1972 Inbetriebnahme INPOL-Fahndungsdatei
- 1975 Gesamtkonzeption INPOL
- Anfang 80er PIOS-Dateien (Personen, Institutionen, Objekte, Sachen), SPUDOK (Spurendokumentationen)
- Seit 1988 Vorbereitungen für INPOL-neu (Grobkonzept 92) flexible Datenformate (Text, Bild, Ton ...), Data-Warehouse-Anwendungen, Führungsinformationen und Auswertungs-Tools
- 2003 Start INPOL-neu, 2006 INPOL-neu 5.0

Entwicklung digitaler Ermittlungsmethoden

Ende 19. Jahrhundert: Daktyloskopie

Weimarer Republik: Telekommunikationsüberwachung

Seit 1958 Fernseh- (Video-) Überwachung

1971-1981 BKA-Präsident Horst Herold: Informatisierung der Kriminalitätsbekämpfung mit elektronischer Ausschreibung, Raster-, Schleierfahndung, Profiling, Aktion Paddy

Ab 1984: genetischer Fingerabdruck

1986: Beginn C-Netz und Mobilkommunikationsüberwachung

Seit 1990 Kommerzialisierung und Überwachung des Internet

Seit 2000 Entschlüsselung des gesamten Humangenoms

Seit 2010 Einsatz von Drohnen

INPOL (seit 1971)

Verbundteilnehmer: BKA, LKÄ, Landespolizeien, Bundespolizei, Zoll mit Grenzkontrollaufgaben, Zollkriminalamt

- Personenfahndung (4,4 Mio.)
- Kriminalaktennachweis (KAN, 4.3 Mio.)
- Innere Sicherheit (früher APIS, 1,5 Mio.)
- Haftdatei (500 T.)
- Violent Crime Linkage Analysis System (ViCLAS)
- DNS-Auskunftsdatei (DAD – Gendatenbank, 800 T.)
- Erkennungsdienst (ED, 5,9 Mio.)
- Automatisiertes Fingerabdruckidentifikationssystem (AFIS-P, 2,5 Mio.)

Data-Warehouse

Beim Data-Warehouse besteht grds. Zweckvielfalt

Vor Einstellung: Qualitätsprüfung erforderlich

- Festlegungen: funktionale Anforderungen, Bedarfsträger, Nutzungsszenarien – im Rahmen der Gesetze
- Datensätze müssen Zweck-Metadaten enthalten (Data-Mart)
- Recherchen in Freitexten und Vorgangsdokumentationen nach definierten Vorgaben (Technik, Dienstvorschriften)
- Rollen- und Aufgabenbeschreibungen: Super-User, normaler Ermittler (nur begrenzt fremde Daten), Sachbearbeiter
- Technische Möglichkeit des Data-Mining

Polizeiliche Zugriffe auf externe Systeme

- Ausländerzentralregister (AZR)
- Automatisierte Fingerabdrücke Ausländer (AFIS-A)
- Bundeszentralregister (BZR beim BAJ)
- Zentrales Verkehrsinformationssystem beim KBA (ZEVIS)
- Bundeszentralamt für Steuern (Kontodaten)
- EURODAC (266 T.)
- SIS (Schengen, z.B. Personenfahndung 110 T.)
- Europäisches Informationssystem (EIS) Europol
- Interpol-Zugriffe über BKA

Länder-IT, Geheimdienst-Kooperation

Länder

- Vorgangsdokumentation (z.B. IGVP Bay, @rtus-VBS SH)
- Viele Spezialdateien (analog Zentral- u. Amtsdateien BKA), z.B. Register Sexualstraftäter, Analyse- und Auswertedateien

Geheimdienstkooperation

- Antiterrordatei, künftig Neo-Nazi-Datei
- Projektdateien

  (Rechtsgrundlage Anti-Terror-Dateigesetz, wird vor dem BVerfG angegriffen)
- Gemeinsame Lagezentren (GIZ, GTAZ, GASIM)

Lokale Schnittstellen

- Zugriff auf (lokale) Melderegister
- Zugriff auf (lokale) Personalausweis-/Passregister
- Kooperation mit Rettungsleitstellen (Feuerwehr, medizinische Notfallversorgung, Katastrophenschutz)
- Kein Zugriff durch Staatsanwaltschaft
- Nutzung für Sicherheitsüberprüfungen, Zuverlässigkeitsüberprüfungen, Einstellungsverfahren

Tendenzen

- Europäisierung: Schengen, Europol, Eurodac, Prüm, Stockholmer Programm, Euro-PNR, Euro-TFTP
- Internationalisierung (u.a. USA, z.B. PNR, SWIFT/TFTP)
- Vergeheimdienstlichung
- Weiterentwicklung der Technik (DNA-Datei, Biometrie, Internetüberwachung, Data-Warehousing, z.B. PIAV)
- Einbeziehung Privater in polizeiliche Ermittlungen (TK, PNR, SWIFT)

Rechtskontrolle digitaler Kriminaltechnik

1. Fach- und Rechtsaufsicht durch Hierarchie und Ministerial-verwaltung
2. Gesetzgebungserfordernis bei Grundrechtseingriff (insbes. nach Volkszählungsurteil 1983 des BVerfG)
3. Parlamentarische nachschauende Kontrolle (Anfragen, Untersuchungs-, Petitions-, Fach- und Sonderausschüsse)
4. Journalistische Kontrolle (Art. 5 GG)
5. Wissenschaftliche Forschung und Diskurs
6. StPO- und Datenschutz-Betroffenenrechte
7. Datenschutzkontrolle
8. Justizielle Prüfung, u. a. durch Bundesverfassungsgericht

Zu 2.) Rechtsgrundlagen

- Grundgesetz: Gewaltenteilung (19 IV, 20, 38, 97) Presse (5)
  Grundrechte (v.a. 10, 2 I iVm 1 I – Recht auf informationelle Selbstbestimmung, Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)

  Einfaches Recht, u.a.
- Bundeskriminalamtsgesetz (BKAG), Bundespolizeigesetz, Zollfahndungsdienstgesetz
- Strafprozessordnung (§§ 474 ff. StPO)
- Landespolizeigesetze
- Bundesdatenschutzgesetz (BDSG) Landesdatenschutzgesetze (LDSG)

Zu 2.) Sicherheitsgesetzgebung

Kommunistenverfolgung zu Zeiten des Kalten Krieges
Notstandsgesetzgebung 1968, Berufsverbote 1972
70er Jahre: RAF u. 1. Welle der Terrorismusgesetzgebung Kontaktsperregesetz, Anfang 90er Jahre: Sicherheitsgesetzgebung (Vorzeichen OK) BVerfSchG, BNDG, MADG, BKAG
Laufende (seit 1968) Ausweitung des TKÜ (§§ 100a ff. StPO)
1998 Zulassung des großen Lauschangriffs (Arg. OK)
Nach 11.09.2001:
Terrorismusbekämpfungsgesetze (Otto I u. II)
Rasterfahndung 2002
Neue Polizeigesetze von Ländern und Bund
2006 TerrBekErgG und AntiterrordateiG
2007 Vorratsdatenspeicherung (vom BVerfG aufgehoben), TKÜ in StPO
2008 BKA-Gesetz mit Online-Durchsuchung
2012 Neonazi-Datei-Gesetz ?

Zu 3.) Parlamentarische Kontrolle

Regelmäßige Berichte über TKÜ, Lauschangriffe u. Ä.

Bsp. Bericht BT-Drs. 17/7307 Präventive Polizeidateien

Bsp. Dez. 2011: Hundertausendfache „stille SMS"

BT-Drs. 17/8257 Computergestützte Kriminaltechnik (bisher nur Anfrage)

Zu 4.) Unabhängige Presse

Von 1975/76 Lauschangriff auf Atomwissenschaftler Traube

1977 Stammheim-Abhör-Affäre

1979 Spiegel-Bölsche Report …

- Umfangreiche und tiefgehende Recherche
- Professionelle Veröffentlichung
- Vertrauliche Quellennutzung (Beschlagnahmeschutz, Zeugnisverweigerungsrecht)

… bis heute, z. B. Echelon ab 1992

2002 Total Information Awareness

2010 INDECT

Zu 5.) Wissenschaft, Initiativen

Forschungs- un Publikationsarbeiten von

- Max-Planck-Institut Freiburg (TKÜ-Gesetzes-Evaluation)
- Universitäten, (Fach-) Hochschulen der Polizei
- Statewatch z.B. zur EU-Strafverfolgung:
  http://www.statewatch.org/analyses/no-145-ecris-epris-ixp.pdf
- Bürgerrechte & Polizei (CILIP)
- Chaos Computer Club (Staatstrojaner)

Zu 6.) Auskunft an Betroffene/Verteidiger

- § 147 StPO: Akteneinsicht des Verteidigers
  nicht bei Gefährdung des Untersuchungszwecks

- Auskunftsanspruch an Betroffene
  Pauschal-Auskunftsverweigerung unzulässig, Einzelfallbegründung nötig
  Bei Verbunddateien Weiterleitungspflicht an verantwortliche Stelle (§ 6 II BDSG) Umsetzung fraglich
  Bei Auskunftsverweigerung Kontrollmöglichkeit durch zuständigen DSB (LfD, BfDI)

Zu 7.) Datenschutzkontrolle

Bearbeitung von Betroffenenbeschwerden + Eingaben

Stellungnahmen u.a. in Öffentlichkeit, gegenüber Gesetzgebern, Verfassungsgerichten

Regelmäßige Tätigkeitsberichte, Kontrollberichte

Entschließungen der DSB-Konferenz

1979: Diskussion über 1. Dateienbericht des BMI …

… bis heute, z.B. 2000: ULD entwickelt Selbstschutz-Tool Anonymisierungsdienst mit, Verschlüsselungshilfen

2005: ULD SH erstmals zu Funkzellenabfrage

Februar 2011: SächsDSB: Funkzellenabfrage in Dresden

Zu 8.) Landesverfassungsgerichte

14.06.1994	SächsVerfGH	SächsPolG
21.10.1999	MVVerfG	Schleierfahndung
18.05.2000	MVVerfG	Gr. Lauschangriff Polizei
10.07.2003	SächsVerfGH	PolG Kontrollpunkte
21.07.2005	SächsVerfGH	Gr. Lauschangriff VerfSch
12.12.2005	HessStGH	Rasterfahndung (Klage unzulässig)
07.02.2006	BayVerfGH	Schleierfahndung
29.01.2007	VerfGH RP	pol. Wohnraumüberwachg. (zulässig)

Zu 8.) Bundesverfassungsgericht

20.06.1984 Strategische Fernmeldeüberwachung
03.03.2004 Gr. Lauschangriff
03.03.2004 AWG Telekommunikationsüberwachung
12.04.2005 GPS-Ortung
27.07.2007 NdsSOG präv. Telekommunikationsüberwachung
04.04.2006 Rasterfahndung
23.02.2007 anlasslose Videoüberwachung
27.02.2008 Heimliche Online-Überwachung (VerfSchG NRW)
11.03.2009 Kfz-Kenzeichen-Erfassung
17.02.2009 Bayerisches Versammlungsgesetz (u.a. Videokontrolle)
22.05.2009 Genetischer Fingerabdruck
11.08.2009 Videoüberwachung Straßenverkehr
02.03.2010 TK-Vorratsdatenspeicherung
Demnächst (?): AntiTerrorDateiG

Zu 8.) Europäische Gerichte

Europäischer Gerichtshof
30.05.2006 US-PNR-Vertrag ohne korrekten Rechtsgrund
16.12.2008 AZR-Diskriminierung
10.02.2009 EG-Vorratsdatenspeicherung (Klage unzulässig)
29.06.2010 EG-Terrorlisten

Europäischer Gerichtshof für Menschenrechte
15.06.1992 Telefonabhöraktion (Deutschland, zulässig)
29.06.2006 Abhören gemäß G-10-Gesetz (Deutschland, zul.)
04.12.2008 DNA-Probenbank (Großbritannien)
10.02.2009 Telefonabhörmaßnahme (Moldawien)
02.09.2010 GPS-Überwachung (Deutschland)

Perspektiven

- Rasante technische Entwicklung und Internationalisierung bei Datenerhebung und -nutzung
- Differenzierte fachspezifische Kontrolle (Relevanz ändert sich laufend)
- Öffentliche Debatte über Einsatz polizeilicher Kriminaltechnik spielt kaum (noch) eine Rolle
- Polizeiliche Datenspeicherung hat angesichts technischer Entwicklungen (IT- und Bio-) sowie Internationalisierung weiterhin höchste Grundrechtsrelevanz
- Rechts- und Kontrollsystem muss in Europa und global ausgebaut werden

Mit Recht und Gesetz gegen ausufernde digitale Kriminaltechnik?

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